# Comptia SY0-401 Exam Questions & Answers

Number: SY0-401
Passing Score: 800
Time Limit: 120 min
File Version: 47.5

**Comptia SY0-401 Exam Questions & Answers**

**Exam Name: CompTIA Security+ Certification Exam**

**Exam A**

**QUESTION 1**
A security administrator wants to implement a more secure way to login to a VPN in addition to a username and password. Which of the following is the MOST secure way to log in to a VPN?

A. Implementing an ACL
B. Setting up a PKI
C. Implementing a single sign on process
D. Setting up two VPNs

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer B

Explanation:
Public key infrastructure , PKI is an encryption system that utilizes a variety of technologies to provide confidentiality, integrity, authentication, and nonrepudiation. PKI uses certificates issued from a CA to provide this capability as well as encryption. PKI is being widely implemented in organizations worldwide.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 371

**QUESTION 2**
Which of the following is the BEST example of a physical security policy?

A. All doors to the server room must have signage indicating that it is a server room.
B. All server room users are required to have unique usernames and passwords.
C. All new employees are required to be mentored by a senior employee for their first few months on the job.
D. New server room construction requires a single entrance that is heavily protected.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: D

Explanation:
It is easier to manage and monitor a single point of enttry which reduces your area of attack.

Source: eMTD

**QUESTION 3**
Which of the following audit types would a security administrator perform on the network to ensure each workstation is standardized?

A. Group policy
B. Domain wide password policy
C. Storage and retention policy
D. User access and rights

**Correct Answer:** A
**Section: (none)**

**Explanation**

**Explanation/Reference:**
Answer: A

Explanation:
With a Group Policy, you create restrictions that will apply to workstations when users authenticate. Upon each authentication, those restrictions are then applied as Registry settings, providing an efficient way to manage a large number of computers.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 229

**QUESTION 4**
Which of the following signature-based monitoring systems is used to detect and remove known worms and Trojans on a host?

A. NIPS
B. Antivirus
C. Anti-spam
D. HIDS

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: B

Explanation:
Antivirus software scans a computer’s memory, disk files, and incoming and outgoing e-mail. The software typically uses a virus definition file that is updated regularly by the manufacturer.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 14
*(A definition file is also known as a signature file)*

**QUESTION 5**
Which of the following is the MOST efficient way to secure a single laptop from an external attack?

A. NIPS
B. HIDS
C. Software firewall
D. Hardware firewall

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
A firewall, sometimes called a packet filter, is designed to prevent malicious packets from entering or leaving computers. A firewall can be software-based or hardware-based. A personal software firewall runs as a program on a local system to protect it against attacks.

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 103

**QUESTION 6**
Disabling the SSID broadcast removes the identifier from which of the following wireless packets?

A. Probe
B. ACK
C. Beacon
D. Data

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
For a degree of protection, some wireless security sources encourage users to configure their APs to prevent the beacon frame from including the SSID but instead require the user to enter the SSID manualJy on the wireless device. Although this may seem to provide protection by not advertising the SSID, in reality it does not, for several reasons.

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 199

**QUESTION 7**
Which of the following describes the role of a proxy server?

A. Analyzes packets
B. Serves as ahoneypot
C. Blocks access to the network
D. Forwards requests for services from a client

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: D

Explanation:
Proxy Server: A type of server that makes a single Internet connection and services requests on behalf of many users..

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 579

**QUESTION 8**
Which of the following is used to both deploy and reapply baseline security configurations?

A. Performance baseline
B. Security agent
C. Security template
D. Configuration baseline

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
A security template is a method to configure a suite of baseline security settings. On a Microsoft Windows computer, one method to deploy security templates is to use Group Policies, a feature that provides centralized management and configuration of computers and remote users who are using specific Microsoft directory services known as Active Directory (AD).

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 336

**QUESTION 9**
Which of the following is BEST suited to detect local operating system compromises?

A. Personal firewall
B. HIDS
C. Anti-spam
D. System log

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: B

Explanation:
A *host-based IDS (HIDS)* is designed to run as software on a host *{local}* computer system. These systems typically run as a service or as a background process. HIDSs examine the machine logs, system events, and applications interactions; they normally don't monitor incoming network traffic to the host.

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 189

**QUESTION 10**
Why is an ad-hoc network a security risk?

A. An ad-hoc network allows access to another computer at the same level of the logged in user, compromising information.
B. An ad-hoc network allows access to the nearest access point which may allow a direct connection to another computer.
C. An ad-hoc network allows access to the nearest access point which may give elevated rights to the connecting user.
D. An ad-hoc network allows access to another computer but with no rights so files cannot be copied or changed.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: A

Explanation:
Similar to 1M in which users connect directly to each other without using a centralized server, a peer-to-peer (P2P) network also uses a direct connection between users. A P2P network does not have servers, so each device simultaneously functions as both a client and a server to all other devices connected to the network. P2P networks are typically used for connecting devices on an ad hoc basis for file sharing of audio, video, and data, or real-time data transmission such as telephony traffic.

Because P2P networks communicate directly between two devices, they are tempting targets for attackers. Viruses, worms, Trojan horses, and spyware can be sent using P2P. Most organizations prohibit P2P communications because of the high risk of infection and legal consequences.

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 99

**QUESTION 11**
Which of the following uses multiple encryption keys to repeatedly encrypt its output?

A. AES256
B. DES
C. 3DES
D. AES128

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
Triple Data Encryption Standard (3DES) was designed to replace DES. As its name implies, 3DES uses three rounds of encryption instead of just one. The ciphertext of one round becomes the entire input for the second iteration. 3DES employs a total of 48 iterations in its encryption (three iterations times 16 rounds). The most secure versions of 3DES use different keys for each round.

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 379

**QUESTION 12**
Which of the following encryption technologies is BEST suited for small portable devices such as PDAs and cell phones?

A. TKIP
B. PGP
C. AES192
D. Elliptic curve

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: D

Explanation:
*Elliptic Curve Cryptography (ECC)* provides similar functionality to RSA. ECC is being implemented in smaller, less-intelligent devices such as cell phones and wireless devices. It's smaller than RSA and requires less computing power. ECC encryption systems are based on the idea of using points on a curve to define the public/private key pair. This process is less mathematically intensive than processes such as RSA.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 326

**QUESTION 13**
Which of the following protocols correspond to port 514 by default?

A. SYSLOG
B. SNMP
C. IMAP
D. FTP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: A

Explanation:
UDP port 514 Syslog Unix system log

Source: Security+ certification exam guide by **Greg White** pg: 84

**QUESTION 14**
Which of the following is achieved and ensured by digitally signing an email?

A. Availability
B. Confidentiality
C. Delivery
D. Integrity

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: A

Explanation:
A *digital signature* is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 328

**QUESTION 15**
Which of the following is BEST used for providing protection against power fluctuation?

A. Generator
B. Voltmeter
C. UPS
D. Redundant servers

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:

An on-line UPS can clean the electrical power before it reaches the server to ensure that a correct and constant level of power is delivered to the server. The UPS can also serve as a surge protector, which keeps intense spikes of electrical current, common during thunderstorms, from reaching systems

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 451

**QUESTION 16**
Which of the following increases availability during periods of electromagnetic interference? (Select TWO).

A. Fiber optic cable
B. Straight-through cable
C. STP cable
D. Crossover cable
E. UTP cable

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answers: A and C

Explanation:
Because fiber-optic cabling uses light in place of an electrical signal, it’s less likely than other implementations to be affected by interference problems.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 153

Shielded twisted-pair (STP) has a foil shield around hte pairs to provide extra shielding from electromagnetic interference.

Source: CompTIA Security+ All-in-One Exam Guide, Second Edition by **Gregory B. White** pg: 220

**QUESTION 17**
A secure company portal, accessible publicly but only to company employees, frequently fails to renew its certificates, resulting in expired certificate warnings for users. These failures: (Select TWO).

A. Increase resources used by the company's web-servers.
B. Expose traffic sent between the server and the user's computer.
C. Breed complacency among users for all certificate warnings.
D. Permit man-in-the-middle attacks to steal users' credentials.

E. Are irritating to the user but the traffic remains encrypted.

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C and E

Explanation:
Most applications that are key enabled or certificate enabled check the expiration date on a key and report to the user if the key has expired. PKI gives the user the opportunity to accept and use the key.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 364

*Since the user would keep getting the pop-up notification of a expired key, they wouldbecome complacent and not read future warnings andjust click to use the key.  If the user accepts to use the key, the data will still be encripted. **eMTD**.

**QUESTION 18**
The last company administrator failed to renew the registration for the corporate web site (e.g. https:// wrtw.comptia.org). When the new administrator tried to register the website it is discovered that the registration is being held by a series of small companies for very short periods of time. This is typical of which of the following?

A. Spoofing
B. TCP/IP hijacking
C. Domain name kiting
D. DNS poisoning

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
Another DNS weakness is *Domain Name Kiting*. When a new domain name is issued, there is a five-day grace period before you must technically pay for it. Those engaged in kiting can delete the account within the five days and re-register it again—allowing them to have accounts that they never have to pay for.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 60

**QUESTION 19**
Which of the following system security threats negatively affects confidentiality?

A. Spam
B. Adware
C. Spyware
D. Worm

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Answer: C

Explanation:
Although spyware is often dismissed as just a nuisance, two characteristics of spyware make it as dangerous as viruses and worms. First unlike the creators of viruses who generally focus on gaining personal notoriety through the malicious software that they create, spyware creators are motivated by profit: their goal is to generate income through spyware advertisements or by acquiring personal information that they can then use to steal from users. Because of this heightened motivation, spY' are is often more intrusive than viruses, harder to detect, and harder to remove. Second, harmful spyware is not always easy to identi.fy. This is because not all software 'that performs one of the functions listed is necessarily spy·ware.

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 51

**QUESTION 20**
Which of the following describes an action taken after a security breach?

A. Disaster recovery planning
B. Business continuity planning
C. Forensic evaluation
D. Change management

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
*Forensics* refers to the process of identifying what has occurred on a system by examining the data trail. *Incident response* encompasses forensics and refers to the process of identifying, investigating, repairing, documenting, and adjusting procedures to prevent another incident. Simply, an *incident* is the occurrence of any event that endangers a system or network.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 192

**QUESTION 21**
Which of the following is true about the application of machine virtualization?

A. Virtualization hosting is only possible on one specific OS.
B. Machine vitalization is only possible in a 64-bit environment.
C. Some malware is able to detect that they are running in a virtual environment.
D. The vitalization host OS must be within two revisions of the guest OS.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
However, if a virtual server on a physical machine is infected, no physical devices exist between it and the other virtual machines. The infected machine then has the potential to quickly infect all other virtual machines on the same physical computer that contain the same vulnerability.

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 61

**QUESTION 22**
All administrators are now required to use 15 character passwords. Which of the following is the BEST method to enforce this new password policy?

A. Email announcements
B. Account expiration configuration
C. Group policy
D. Forcing all users to change their password on next login

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
Within the Windows OS's, security templates can contain hundreds of settings that control or modify settings on the system such as password lenght, auditing of a user actions, or restrictions on network access. Security templates can be standalone files that are applied manually to each system, but they can also be part of a group policy, allowing common security settings to be applied ro the systems on a much wider scale.

Source: CompTIA Security+ All-in-One Exam Guide, Second Edition by **Gregory B. White** pg: 384

**QUESTION 23**
Management has requested increased visibility into how threats might affect their organization. Which of the following would be the BEST way to meet their request without attempting to exploit those risks?

A. Conduct a penetration test.
B. Conduct a risk assessment.
C. Conduct a social engineering test.
D. Conduct a security awareness seminar.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: B

Explanation:
*Risk assessment* (or *risk analysis*) The process of analyzing an enviorment to identify the threats, vulnerabilities, and mitigation actions to determine (either quantitatively or qualitatively) the impact of an event that would affect a project, program, or business.

Source: Security+ certification exam guide by **Greg White** pg: 478

**QUESTION 24**
Which of the following stores information with a trusted agent to decrypt data at a later date, even if the user destroys the key?

A. Key registration
B. Recovery agent

C. Key escrow

D. Public trust model

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
*Key* escrow refers to a situation in which keys are managed by a third party, such as a trusted CA. In key escrow, the private key is split and each half is encrypted. The two halves are sent to the third party, which stores each half in a separate location. A user can then retrieve the two halves, combine them, and use this new copy of the private key for decryption. Key escrow relieves the end user from the worry of losing her private key.

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 418

**QUESTION 25**
Which of the following will help hide the IP address of a computer from servers outside the network?

A. NAT

B. PAT

C. ACL

D. NAC

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: A

Explanation:
NAT effectively hides your network from the world, making it much harder to determine what systems exist on the other side of the router. The NAT server effectively operates as a firewall for the network. Most new routers support NAT; it provides a simple, inexpensive firewall for small networks.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 31

**QUESTION 26**
When developing a new firewall policy, which of the following methods provides the MOST secure starting point?

A. Implicit deny

B. Least privilege

C. Stateful inspection

D. Due diligence

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: A

Explanation:
Implicit deny in access control means that if a condition is not explicitly met, then it is to be rejected. *(Implicit* means that something is implied or indicated but not actually expressed.) For example, a router may have a rule-based access control restriction. Yet if no conditions match the restrictions, the router rejects access because of an implicit *deny all* clause: any action that is not explicitly permitted is denied. When creating access control restrictions it is recommended that unless the condition is specificaUy met, then it should be denied.

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 234

**QUESTION 27**
An administrator is required to keep certain workstations free of malware at all times, but those workstations need to be able to access any Internet site. Which of the following solutions would be the BEST choice?

A. Updated antivirus software
B. Pop-up blockers
C. Personal firewall
D. Updated anti-spam software

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: A

Explanation:
The best initial protection against malicious code is antivirus software.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 492

**QUESTION 28**
Which of the following combinations of items would constitute a valid three factor authentication system?

A. Password, retina scan, and a one-time token
B. PIN, password, and a thumbprint
C. PKI smartcard, password and a one-time token
D. Fingerprint, retina scan, and a hardware PKI token

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: A

Explanation:
One-, two-, and three-factor
authentication merely refers to the number of items a user must supply to authenticate. Authentication can be based on something they have (a smart card), something they know (a password), something unique (biometric), and so forth. After factor authentication is done, then single sign-on can still apply throughout the user’s session.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 415

**QUESTION 29**
Which of the following BEST describes a tool used to encrypt emails in transit?

A. Whole disk encryption
B. SSL over VPN
C. Digital signatures
D. S/MIME certificates

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: D

Explanation:
Secure Multipurpose Internet Mail Extensions (S/MIME) is a standard used for encrypting e-mail. S/MIME contains signature data. It uses the PKCS #7 standard (Cryptographic Message Syntax Standard) and is the most widely supported standard used to secure e-mail communications.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 351

**QUESTION 30**
Which of the following security threats would MOST likely use IRC?

A. Botnets
B. Adware
C. Logic bombs
D. Spam

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: A

Explanation:
One of the popular payloads of malware today that is carried by Trojan horses, worms, and viruses is a program that will allow the infected computer to be placed under the remote control of an attacker. This infected "robot" computer is known as a zombie. When hundreds, thousands, or even tens of thousands of zombie computers are under the control of an attacker, this creates a botnet. Attackers use Internet Relay Chat (IRC) to remotely control the zombies. IRC is an open communication protocol that is used for real-time "chatting" with other IRC users over the Internet.

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 54

**QUESTION 31**
Which of the following tools will detect protocols that are in use?

A. Spoofing
B. Port scanner
C. Proxy server
D. DMZ

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: B

Explanation:
The item (physical or software) that scans a server for open ports that can be taken advantage of. Port scanning is the process of sending messages to ports to see which ones are available and which ones aren't.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 577

**QUESTION 32**
An auditor would use credentials harvested from a SQL injection attack during which of the following?

A. Forensic recovery
B. Vulnerability assessment
C. Penetration test
D. Password strength audit

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
A penetration test is the best way to tell what services are really running on your system. *Penetration testing* involves trying to get access to your system from an attacker's perspective. Typically, you perform this test from a system on the Internet and try to see if you can break in or, at a minimum, get access to services running on your system.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 222

*The key word in the question is "aduitor". Had it said "attacker" then I think A would be the correct answer.
**eMTD**

**QUESTION 33**
Key escrow is the process of:

A. Entrusting the keys to a third party.
B. Backing up the key to local storage.
C. Removing the public key.
D. Removing the private key.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: A

Explanation:
A key escrow system stores keys for the purpose of law enforcement access. One of the proposed methods of dealing with key escrow involves the storage of key information with a third party, referred to as a key escrow

agency .

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 363

**QUESTION 34**
Which of the following will allow a technician to restrict access to one folder within a shared folder?

A. NTLM
B. IPSec
C. NTLMv2
D. NTFS

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: D

Explanation:
With NTFS, files, directories, and volumes can each have their own security. NTFS's security is flexible and built in. Not only does NTFS track security in access control lists (ACLs), which can hold permissions for local users and groups, but each entry in the ACL can specify what type of access is given—such as Read-Only, Change, or Full Control.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 234

**QUESTION 35**
A data entry technician uses an application from the Internet to gain administrative rights on a system. Gaining unauthorized domain rights is an example of:

A. A logic bomb.
B. Arootkit.
C. Spyware.
D. Privilege escalation.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: D

Explanation:
Operating systems and many applications have the ability to restrict a user's privileges in accessing its specific functions. Privilege escalation is exploiting a vulnerability in software to gain access to resources that the user would normally be restricted from obtaining.

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 47

**QUESTION 36**
Which of the following would be implemented to provide a check and balance against social engineering attacks?

A. Password policy
B. Single sign-on

C. Separation of duties
D. Biometric scanning

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
Separation of duties helps prevent an individual from embezzling money from a company. To successfully embezzle funds, an individual would need to recruit others to commit an act of *collusion* (an agreement between two or more parties established for the purpose of committing deception or fraud). Collusion, when part of a crime, is also a criminal act in and of itself.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 410

**QUESTION 37**
A NIPS is primarily used for which of the following purposes?

A. To monitor network traffic in promiscuous mode
B. To alert the administrator to known anomalies
C. To log any known anomalies
D. To take action against known threats

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: D

Explanation:
As opposed to *Network Intrusion Detection Systems (NIDSs), Network Intrusion Prevention Systems (NIPSs)* focus on *prevention*. These systems focus on signature matches and then take a course of action. For example, if it appears as if an attack might be underway, packets can be dropped, ignored, and so forth. In order to be able to do this, the NIPS must be able to *detect* the attack occurring, and thus it can be argued that NIPS is a subset of NIDS.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 190

**QUESTION 38**
Which of the following algorithms provides the LOWEST level of encryption?

A. SHA1
B. Blowfish
C. DES
D. AES

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
The *Data Encryption Standard (DES)* has been used since the mid-1970s. It was the primary standard used in government and industry until it was replaced by AES. It's a strong and efficient algorithm based on a 56-bit key. (*Strong* refers to the fact that it's hard to break.) A recent study showed that a very powerful system could break the algorithm in about two days. DES has several modes that offer security and integrity. However, it has become a little dated as a result of advances in computer technology, and it's being replaced. For its time, it was one of the best standards available.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 323

**QUESTION 39**
At midnight on January 1st, an administrator receives an alert from the system monitoring the servers in the datacenter. All servers are unreachable. Which of the following is MOST likely to have caused the DOS?

A. Rootkit
B. Virus
C. Logic bomb
D. Botnet

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: C

Explanation:
*Logic bombs* are programs or snippets of code that execute when a certain predefined event occurs. A bomb may send a note to an attacker when a user is logged on to the Internet and is using a word processor. This message informs the attacker that the user is ready for an attack.

Logic bombs may also be set to go off on a certain date or when a specified set of circumstances occurs.

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 88

**QUESTION 40**
Which of the following would an auditor use to determine if an application is sending credentials in clear text?

A. Vulnerability scanner
B. Protocol analyzer
C. Rainbow table
D. Port scanner

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: B

Explanation:
A protocal analyzer (also known as a packet sniffer, network analyzer, or network sniffer) is a peice of software or an integrated software/hardware stsyem that can capture and decode network traffic. ... From a security prospective, protocal analyzers can be used for a number of activities, such as the following:... Testing encryption between systems or applications.

Source: CompTIA Security+ All-in-One Exam Guide, Second Edition by **Gregory B. White** pg: 329

**QUESTION 41**
Which of the following security controls targets employee accounts that have left the company without going through the proper exit process?

A. Password complexity policy
B. Account expiration policy
C. Account lockout policy
D. Access control lists

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: B

Explanation:
To assist with controlling orphaned accounts, account expiration can be used, Account expiration is the process of setting a user's account to expire. Account expiration is not the same as password expiration. Account expiration indicates when an account is no longer active; password expiration sets the time when a user must create a new password in order to access his account,

Source: SECURITV+ GUIDE TO NETWORK SECURITY FUNDAMENTALS THIRD EDITION by **MARK CIAMPA** pg: 238

**QUESTION 42**
Which of the following logs would MOST likely indicate that there is an ongoing brute force attack against a servers local administrator account?

A. Firewall
B. System
C. Performance
D. Access

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer: B

Explanation:
Audit files and system logs are very effective for tracking activity in a network or on a server. They should be reviewed regularly to identify if unauthorized activity is occurring. Systems should be routinely inspected to verify whether physical security procedures are being followed

Source: Sybex CompTIA Securit+ Delux Study Guide by **Emmett Dulaney** pg: 95

**QUESTION 43**
Which of the following security concepts is supported by HVAC systems?

A. Availability
B. Integrity
C. Confidentiality
D. Privacy

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Anwser: A

Explanation:
HVAC is an acronym for heating, ventalation, and air conditioning. It is the control system used  to control humidty, tempature, and air flow. The enviorment in server rooms and other areas where sensitive equipment resides needs to have controlled conditions to operate properly. If tempatures or humidity are too high or too low, it can damage the equipment and result in the loss of data.

Source: CompTIA Security+: Exam SYO 201, Study Guide and Prep Kit by **Ido Dubrawsky** pg: 566

## Exam B

**QUESTION 1**
Which of the following can be implemented to mitigate the risks associated with open ports on a server?

A. Enable MAC filtering
B. Implement a password policy
C. Disable unnecessary programs
D. Disable network cards

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 2**
After a disaster, a security administrator is helping to execute the company disaster recovery plan. Which of the following security services should be restored FIRST?

A. Auditing and logging of transactions.
B. Authentication mechanisms for guests.
C. Help desk phones and staffing.
D. New user account creation services.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 3**
Which of the following security concerns stern from the use of corporate resources on cell phones? (Select TWO).

A. Cell phones are easily lost or stolen.
B. MITM attacks are easy against cell phones.
C. There is no antivirus software for cell phones.
D. Cell phones are used for P2P gaming.
E. Encryption on cell phones is not always possible.

**Correct Answer:** AE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
A user notices that in the morning the email system is slow. Which of the following tools would the technician use FIRST to identify the issue?

A. Protocol analyzer

B. VPN
C. Performance monitor
D. Spam filter

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
Which of the following should be disabled to help prevent boot sector viruses from launching when a computer boots?

A. SNMP
B. DMZ
C. USB
D. Hard Drive

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
Which of the following technologies will ensure the datacenter remains operational until backup power can be obtained?

A. UPS
B. Transfer switch
C. Circuit breaker
D. Backup generator

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
A UPS will allow you to continue to function in the absence of power for only a short duration. For fault tolerance in situations of longer duration, you will need a backup generator. Backup generators run off of gasoline or diesel and generate the electricity needed to provide steady power.

**QUESTION 7**
In a standard PKI implementation, which of the following keys is used to sign outgoing messages?

A. Sender's private key
B. Recipient's public key
C. Sender's public key
D. Recipient's private key

**Correct Answer:** A

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
The security administrator is investigating a breach of the company's web server. One of the web developers had posted valid credentials to a web forum while troubleshooting an issue with a vendor. Logging which of the following would have created the BEST way to determine when the breach FIRST occurred? (Select TWO).

A. Unsuccessful login
B. Source OS
C. Destination IP
D. Number of hops from source
E. Source IP
F. Successful login

**Correct Answer:** EF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 9**
Which of the following would be MOST useful for a security technician to run on a single, stand- alone machine with no network interface to verify its overall security posture?

A. Password cracker
B. Protocol analyzer
C. Networkmapper
D. Port scanner

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 10**
One of the primary purposes of visualization in a data center is to reduce which of the following?

A. Volume of physical equipment needing to be secured
B. Total complexity of the overall security architecture
C. Number of logical hosts providing services for users
D. Amount of application logging required for security

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
Patches and updates should be applied to production systems:

A. After vetting in a test environment that mirrors the production environment.
B. As soon as the vendor tests and makes the patch available.
C. After baselines of the affected systems are recorded for future comparison.
D. As soon as the Configuration Control Board is alerted and begins tracking the changes.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
On network devices where strong passwords cannot be enforced, the risk of weak passwords is BEST mitigated through the use of which of the following?

A. Limited logon attempts
B. Removing default accounts
C. Reverse proxies
D. Input validation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
Which of the following can ensure the integrity of email?

A. MD5
B. NTLM
C. Blowfish
D. LANMAN

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
Which of the following allows management to track whether staff members have accessed an authorized area?

A. Physical tokens
B. Physical access logs
C. Man-traps
D. Hardware locks

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
Which of the following is used to provide a fixed-size bit-string regardless of the size of the input source?

A. SHA
B. 3DES
C. PGP
D. WEP

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 16**
A new application support technician is unable to install a new approved security application on a departmental's workstation. The security administrator needs to do which of the following?

A. Add that user to the local power users group
B. Add that user to the domain administrators group
C. Add that user to the domain remote desktop group
D. Add that user to the security distribution group

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
Which of the following is a goal of penetration testing?

A. Passively assess web vulnerabilities
B. To check compliance of the router configuration
C. Provide a passive check of the network's security
D. Actively assess deployed security controls

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
The firewall administrator sees an outbound connection on IP port 50 and UDP port 500. Which of the following is the cause?

A. IPSec VPN connection
B. SSH tunneling
C. Certificate revocation list look-up
D. Incorrect DNS setup

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 19**
A penetration tester is attempting to run a brute-force attack to discover network passwords. Which of the following tools would be BEST suited to this task?

A. John the Ripper
B. Metasploit
C. OVAL
D. Milw0rm

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords.

**QUESTION 20**
A user reports that they cannot print anything from the file server or off the web to the network printer. No other users are having any problems printing. The technician verifies that the user's computer has network connectivity. Which of the following is the MOST probable reason the user cannot print?

A. The printer is not setup up correctly on the server.
B. The user does not have full access to the file server.
C. The user does not have Internet access.
D. The user does not have access to the printer.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
A remote network administrator calls the helpdesk reporting that they are able to connect via VPN but are unable to make any changes to the internal web server. Which of the following is MOST likely the cause?

A. IPSec needs to be reinstalled on the administrator's workstation.
B. The administrator needs to be added to the web server's administration group.

C. The VPN concentrator needs to be configured.

D. The administrator does not have the correct access rights to dial in remotely.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
A security administrator has reports of an employee writing harassing letters on a workstation, but every time the security administrator gets on the workstation there is no evidence of the letters. Which of the following techniques will allow the security administrator to acquire the necessary data?

A. VLAN

B. Memory forensics

C. Firewall

D. Dumpster diving

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
An administrator needs to implement a backup strategy that provides the fastest recovery in case of data corruption. Which of the following should the administrator implement?

A. Fullbackup on Sunday and differential backups every other day

B. Fullbackup on Sunday and incremental backups every other day

C. Fullbackup on Sunday and a full backup every day

D. Fullbackup on Sunday and alternating differential and incremental every other day

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
A network administrator places a firewall between a file server and the public Internet and another firewall between the file server and the company's internal servers. This is an example of which of the following design elements?

A. DMZ

B. Subnetting

C. VLAN

D. NAT

**Correct Answer:** A
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 25**
Which of the following security attacks would be MOST likely to occur within the office without the use of technological tools?

A. Phishing
B. Cold calling
C. Shoulder surfing
D. SPIM

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
One form of social engineering is known as shoulder surfing and involves nothing more than watching someone when they enter their sensitive data. They can see you entering a password, typing in a credit card number, or entering any other pertinent information. The best defense against this type of attack is simply to survey your environment before entering personal data.

**QUESTION 26**
Which of the following is a service that provides authentication, authorization and accounting to connecting users?

A. LANMAN
B. WPA
C. RADIUS
D. CHAP

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 27**
Which of the following would MOST likely monitor user web traffic?

A. A proxy server
B. Enable cookie monitoring
C. A software firewall
D. Enable Internet history monitoring

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
Which of the following uses a trusted third party key distribution center to generate authentication tokens?

A. TACACS
B. CHAP
C. LDAP
D. Kerberos

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
Which of the following can be used to prevent ongoing network based attacks?

A. NIDS
B. HIDS
C. NAT
D. NIPS

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**
Regression testing and deployment are part of the:

A. Least privilege principle.
B. Vulnerability assessment process.
C. Patch management process.
D. Disaster recovery process.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**
A user reports that they opened an attachment from an email received through a distribution list. At a later date, several computers started behaving abnormally. Which of the following threats has MOST likely infected the computer?

A. Pop-ups
B. Spyware
C. Spam
D. Logic bomb

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**
A technician notices that folder permissions are changing randomly on the server. Which of the following tools would the technician use to identify the issue?

A. System monitor
B. DMZ
C. Firewall
D. Protocol analyzer

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**
Which of the following protocols allows a user to selectively encrypt the contents of an email message at rest?

A. SSL/TLS
B. Digital signature
C. Secure SMTP
D. S/MIME

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
A technician completes a WLAN audit and notices that a number of unknown devices are connected. Which of the following can BEST be completed to mitigate the issue?

A. Replace the wireless access point
B. Replace the firewall
C. Change the SSID
D. Enable MAC filtering

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
A company sets up wireless access points for visitors to use wireless devices. Which of the following encryption

methods should they implement to provide the highest level of security?

A. SHA-256
B. WEP
C. WPA2
D. WPA

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 36**
Which of the following would a security administrator be MOST likely to use if a computer is suspected of continually sending large amounts of sensitive data to an external host?

A. Performance baseline
B. Virus scanner
C. Honeypot
D. Protocol analyzer

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
Which of the following contains a list of certificates that are compromised and invalid?

A. CA
B. CRL
C. TTP
D. RA

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
Certificate revocation is the process of revoking a certificate before it expires. A certificate may need to be revoked because it was stolen, an employee moved to a new company, or someone has had their access revoked. A certificate revocation is handled either through a Certificate Revocation List (CRL).

**QUESTION 38**
Which of the following is part of the patch management process?

A. Documenting the security assessment and decision.
B. Reverse engineering non-vendor supplied patches.
C. Examining firewall and NIDS logs.
D. Replacing aging network and computing equipment.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 39**
Which of the following methods allows the administrator to create different user templates to comply with the principle of least privilege?

A. Rule-based access control
B. Mandatory access control
C. Physical access control
D. Role-based access control

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**
Which of the following processes describes identity proofing?

A. Access control and identity verification
B. Identification and non-repudiation
C. Identification and authentication
D. Authentication and authorization

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**
In order for an organization to be successful in preventing fraud from occurring by a disgruntled employee, which of the following best practices should MOST likely be in place?

A. Job rotation
B. Least privilege
C. Separation of duties
D. Access controls

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 42**

A web server that the employees use to fill out their time cards needs to be protected. The web server needs to be accessible to employees both inside the campus and at remote sites. Some of the employees use computers that do not belong to the company to do their work. Which of the following would BEST protect the server?

A. Place the server in a DMZ and require all users to use the company's VPN software to access it.
B. Place the server in a subnet that is blocked at the firewall.
C. Place the server in a DMZ after hardening the OS.
D. Require all users to use a PKI token stored on a physical smart card to authenticate to the server.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 43**
The security administrator wants to know if a new device has any known issues with its available applications. Which of the following would be BEST suited to accomplishing this task?

A. Vulnerability scanner
B. Port scanner
C. Networkmapper
D. Protocol analyzer

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 44**
Which of the following are BEST practices in regards to backup media? (Select TWO).

A. Format tapes annually.
B. Keep the tapes user accessible.
C. Store tapes near the servers.
D. Storebackup's off site.
E. Label the media.

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**Exam C**

**QUESTION 1**
During an annual risk assessment, it is discovered the network administrators have no clear timeline of when patches must be installed. Which of the following would BEST solve this issue?

A. Creating and disseminating a patch management policy
B. Report the issue to management and revisit it during the next risk assessment
C. Training network administrators on the importance of patching
D. Hiring more administrators to better assist in the patching of servers

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 2**
Which of the following is an advanced security tool used by security administrators to divert malicious attacks to a harmless area of the network?

A. Firewall
B. TCP/IP hijacking
C. Proxy server
D. Honeypot

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 3**
Which of the following would be the BEST course of action to maintain network availability during an extended power outage?

A. Install UPS units on each critical device
B. Implement a SONET ring
C. Install backup generators
D. Use multiple servers for redundancy

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
When investigating data breaches caused by possible malicious action, it is important for members of the CIRT to document the location of data at all times. Which of the following BEST describes what the CIRT is trying to document?

A. Proper authorization procedures

B. Disaster recovery plan
C. Chain of custody
D. Damage mitigation

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

A. Restore a random file.
B. Perform a full restore.
C. Read the first 512 bytes of the tape.
D. Read the last 512 bytes of the tape.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
Which of the following groups should be able to view the results of the risk assessment for an organization? (Select TWO).

A. HR employees
B. Information security employees
C. All employees
D. Executive management
E. Vendors

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 7**
Which of the following does a risk assessment include?

A. Exploits, attacks, and social engineering
B. Threats, vulnerabilities, and asset values
C. Management, cost, and budget
D. Policies, procedures, and enforcement

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
Identification is the process of verifying which of the following?

A. The user or computer system
B. The user's access level
C. The uniqueness of a user's token
D. The association of a user

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 9**
Which of the following behavioral biometric authentication models should a technician deploy in a secure datacenter?

A. Voice recognition
B. Fingerprint recognition
C. Iris scan
D. Retina scan

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 10**
Which of the following is a tactic used by malicious domain purchasing organizations?

A. ARP spoofing
B. Kiting
C. DNS
D. DDoS

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
Which of the following would allow an administrator to perform internal research on security threats and common viruses on multiple operating systems without risking contamination of the production environment?

A. AVLAN
B. A firewall

C. A virtual workstation
D. A honey pot

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
Which of the following environmental controls would require a thermostat within the datacenter?

A. Airflowcontrol
B. Moisture control
C. Temperature control
D. Fire suppression

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
A server needs to be configured to allow the sales department ability to read and write a file. Everyone else in the company only needs read access. Which of the following access control lists will do this?

A. Sales: Read=Allow; Write=Allow
Everyone: Read=Allow; Write=None
B. Sales: Read=Allow; Write=Allow
Everyone: Read=Deny; Write=Deny
C. Sales: Read=None; Write=Allow
Everyone: Read=Allow; Write=Allow
D. Sales: Read=Allow; Write=Allow
Everyone: Read=None; Write= None

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
An administrator wants to make sure that all users of a large domain are restricted from installing software. Which of the following should MOST likely be done?

A. A security policy template is implemented
B. A security IP audit is completed
C. Administrative rights are manually removed
D. All workstations are rebuilt

**Correct Answer:** A

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
Which of the following is MOST likely the reason why a security administrator would run a NMAP report on an important server?

A. To correlate which MAC addresses are associated with aswitchport
B. To identify vulnerabilities in available services
C. To determine open ports and services
D. To capture network packets for analysis

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 16**
Which of the following should be done if a USB device is found in a parking lot?

A. Call the manufacturer of the USB device.
B. Plug it in to a computer to see who it belongs to.
C. Turn it in to the appropriate security person.
D. Reformat it for personal use at home.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
Proper planning for disaster recovery includes which of the following?

A. Testing the plan on a regular basis
B. Having system administrators electronically sign the plan
C. Documenting all HDD serial numbers
D. Executing the continuity plan at random

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
Using a digital signature during an online transaction is a form of:

A. Key management.

B. Availability.
C. Confidentiality.
D. Non-repudiation.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 19**
Which of the following is MOST likely to occur if the input of a web form is not properly sanitized? (Select TWO).

A. SQL injection
B. Backendfile system crash
C. Web load balancing
D. Cross-site scripting
E. Logic bomb

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
Rainbow tables are primarily used to expose which of the following vulnerabilities?

A. Available ports
B. Weak encryption keys
C. Weak passwords
D. Available IP addresses

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
Which of the following devices would be used to gain access to a secure network without affecting network connectivity?

A. Router
B. Vampire tap
C. Firewall
D. Fiber-optic splicer

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
Which of the following can increase risk? (Select TWO).

A. Vulnerability
B. Mantrap
C. Configuration baselines
D. Threat source
E. Mandatory vacations

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
Which of the following is the MOST secure way to encrypt traffic and authenticate users on a wireless network?

A. WPA2 encryption using a RADIUS server
B. WEP encryption using a pre-shared key (PSK)
C. WEP encryption using a RADIUS server
D. WPA2 encryption using a pre-shared key (PSK)

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
Which of the following is MOST likely to be an issue when turning on all auditing functions within a system?

A. Flooding the network with all of the log information
B. Lack of support for standardized log review tools
C. Too much information to review
D. Too many available log aggregation tools

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 25**
Which of the following practices improves forensic analysis of logs?

A. Ensuring encryption is deployed to critical systems.
B. Ensuring SNMP is enabled on all systems.

C. Ensuring switches have a strong management password.

D. Ensuring the proper time is set on all systems.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 26**
A user reports that they cannot download an application from a website on the Internet. Which of the following logs is MOST likely to contain the cause of this problem?

A. Application logs

B. Antivirus logs

C. Firewall logs

D. System logs

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 27**
Which of the following methods assists in determining if user permissions are following the principle of least privilege?

A. Penetration test

B. User rights audit

C. Physical security assessment

D. Vulnerability assessment

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
Which of the following combinations of items would constitute a valid three factor authentication system?

A. Password, retina scan, and a one-time token

B. PIN, password, and a thumbprint

C. PKI smartcard, password and a one-time token

D. Fingerprint, retina scan, and a hardware PKI token

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
In a standard PKI implementation, which of the following keys is used to sign outgoing messages?

A. Senders private key
B. Recipients public key
C. Senders public key
D. Recipients private key

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**
Which of the following should a technician deploy to detect malicious changes to the system and configuration?

A. Pop-up blocker
B. File integrity checker
C. Anti-spyware
D. Firewall

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**
Which of the following asymmetric algorithms was designed to provide both encryption and digital signatures?

A. Diffie-Hellman
B. DSA
C. SHA
D. RSA

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**
Which of the following would be used to look for suspicious processes?

A. System monitor
B. Networkmapper
C. TACACS
D. Protocol analyzer

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**
Which of the following protocols is considered more secure than SSL?

A. TLS
B. WEP
C. HTTP
D. Telnet

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
Which of the following controls would require account passwords to be changed on a regular basis?

A. Password complexity requirements
B. Logical tokens
C. Domain group policy
D. Account expiration

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
Why do security researchers often use virtual machines?

A. To offer an environment where new network applications can be tested
B. To offer a secure virtual environment to conduct online deployments
C. To offer a virtual collaboration environment to discuss security research
D. To offer an environment where malware can be executed with minimal risk to equipment and software

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 36**
Which access control system allows the system administrator to establish access permissions to network resources?

A. MAC
B. DAC
C. RBAC
D. None of the above.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
Which of the following access control models uses roles to determine access permissions?

A. MAC
B. DAC
C. RBAC
D. None of the above.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 38**
Given: John is a network administrator. He advises the server administrator of his company to implement whitelisting, blacklisting, closing-open relays and strong authentication techniques.
Question: Which threat is being addressed?

A. Viruses
B. Adware
C. Spam
D. Spyware

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 39**
Most current encryption schemes are based on

A. digital rights management
B. time stamps
C. randomizing
D. algorithms

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**
Study the following items carefully, which one will permit a user to float a domain registration for a maximum of five days?

A. Spoofing
B. DNS poisoning
C. Domain hijacking
D. Kiting

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**Exam D**

**QUESTION 1**
The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. The public key infrastructure is based on which encryption schemes?

A. Symmetric
B. Quantum
C. Asymmetric
D. Elliptical curve

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 2**
How is access control permissions established in the RBAC access control model?

A. The system administrator.
B. The owner of the resource.
C. The role or responsibilities users have in the organization.
D. None of the above.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 3**
What does the DAC access control model use to identify the users who have permissions to a resource?

A. Predefined access privileges.
B. The role or responsibilities users have in the organization
C. Access Control Lists
D. None of the above.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
Which of the following would allow an administrator to find weak passwords on the network?

A. A networkmapper
B. A hash function
C. A password generator

D. A rainbow table

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
When power must be delivered to critical systems, which of the following is a countermeasure?

A. Backup generator
B. Warm site
C. Redundant power supplies
D. Uninterruptible power supplies (UPSs)

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
Which of the following statements are true regarding File Sharing?

A. FTP is a protocol, a client, and a server.
B. Security was based on the honor system.
C. As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server.
D. When files are stored on a workstation, the connection is referred to as a peer-to-peer connection.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 7**
Which of the following describes a type of algorithm that cannot be reversed in order to decode the data?

A. Symmetric
B. One Way Function
C. Asymmetric
D. Pseudorandom Number Generator (PRNG)

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**

Secret Key encryption is also known as:

A. symmetrical
B. replay
C. one way function.
D. asymmetrical

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 9**
Virtualized applications, such as virtualized browsers, can protect the underlying operating system from which of the following?

A. Malware installation from suspects Internet sites
B. DDoS attacks against the underlying OS
C. Man-in-the-middle attacks
D. Phishing and spam attacks

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 10**
What does the MAC access control model use to identify the users who have permissions to a resource?

A. Predefined access privileges.
B. The role or responsibilities users have in the organization
C. Access Control Lists
D. None of the above

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
Which of the following statements regarding the MAC access control models is TRUE?

A. The Mandatory Access Control (MAC) model is a dynamic model.
B. In the Mandatory Access Control (MAC) the owner of a resource establishes access privileges to that resource.
C. In the Mandatory Access Control (MAC) users cannot share resources dynamically.
D. The Mandatory Access Control (MAC) model is not restrictive.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
Which description is correct about an application or string of code that could not automatically spread from one system to another but is designed to spread from file to file?

A. Botnet
B. Adware
C. Worm
D. Virus

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
In computer security, an access control list (ACL) is a list of permissions attached to an object.
Which log will reveal activities about ACL?

A. Performance
B. Mobile device
C. Firewall
D. Transaction

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
For the following options, which is an area of the network infrastructure that allows a technician to put public facing systems into it without compromising the entire infrastructure?

A. VLAN
B. VPN
C. NAT
D. DMZ

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
Remote authentication allows you to authenticate Zendesk users using a locally hosted script. Which of the following is an example of remote authentication?

A. A user on a metropolitan area network (MAN) accesses a host by entering a username and password pair while not connected to the LAN.
B. A user on a campus area network (CAN) connects to a server in another building and enters a username and password pair.
C. A user in one building logs on to the network by entering a username and password into a host in the same building.
D. A user in one city logs onto a network by connecting to a domain server in another city.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 16**
Documentation describing a group expected minimum behavior is known as:

A. the need to know
B. acceptable usage
C. the separation of duties
D. a code of ethics

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
The CEO of your company is worrying about staff browsing inappropriate material on the Internet via HTTPS. Your company is advised to purchase a product which can decrypt the SSL session, scan the content and then repackage the SSL session without staff knowing. Which type of attack is similar to this product?

A. TCP/IP hijacking
B. Replay
C. Spoofing
D. Man-in-the-middle

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
Sending a patch through a testing and approval process is an example of which option?

A. Acceptable use policies
B. Change management
C. User education and awareness training
D. Disaster planning

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 19**
Choose the access control model that allows access control determinations to be performed based on the security labels associated with each user and each data item.

A. MACs (Mandatory Access Control) method
B. RBACs (Role Based Access Control) method
C. LBACs (List Based Access Control) method
D. DACs (Discretionary Access Control) method

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
For the following items, which is a security limitation of virtualization technology?

A. A compromise of one instance will immediately compromise all instances.
B. It increases false positives on the NIDS.
C. Patch management becomes more time consuming.
D. If an attack occurs, it could potentially disrupt multiple servers.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
What technology is able to isolate a host OS from some types of security threats?

A. Kiting
B. Virtualization
C. Cloning
D. Intrusion detection

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
Which of the following is the BEST place to obtain a hotfix or patch for an application or system?

A. An email from the vendor
B. A newsgroup or forum
C. The manufacturer's website
D. A CD-ROM

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
Tom is a network administrator of his company. He guesses that PCs on the internal network may be acting as zombies participating in external DDoS attacks. Which item will most effectively confirm the administrators?? suspicions?

A. AV server logs
B. HIDS logs
C. Proxy logs
D. Firewall logs

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
Choose the terminology or concept which best describes a (Mandatory Access Control) model.

A. Lattice
B. Bell La-Padula
C. BIBA
D. Clark and Wilson

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 25**

Password cracking tools are available worldwide over the Internet. Which one of the following items is a password cracking tool?

A. Wireshark
B. Nessus
C. John the Ripper
D. AirSnort

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 26**
IDS is short for Intrusion Detection Systems. Which option is the MOST basic form of IDS?

A. Signature
B. Statistical
C. Anomaly
D. Behavioral

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 27**
Which of the following statements is TRUE regarding the Security Token system?

A. If your token does not grant you access to certain information, that information will either not be displayed or your access will be denied. The authentication system creates a token every time a user or a session begins. At the completion of a session, the token is destroyed.
B. A certificate being handed from the server to the client once authentication has been established. If you have a pass, you can wander throughout the network. BUT limited access is allowed.
C. The authentication process uses a Key Distribution Center (KDC) to orchestrate the entire process. The KDC authenticates the network. Principles can be users, programs, or systems. The KDC provides a ticket to the network. Once this ticket is issued, it can be used to authenticate against other principles. This occurs automatically when a request or service is performed by another network.
D. The initiator sends a logon request from the client to the server. The server sends a challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and if the information matches, the server grants authorization.
If the response fails, the session fails and the request phase starts over

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
Which statement is true about the cryptographic algorithm employed by TLS to establish a session key?

A. Blowfish
B. Diffie-Hellman
C. IKE
D. RSA

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
To aid in preventing the execution of malicious code in email clients, which of the following should be done by the email administrator?

A. Spam and anti-virus filters should be used
B. Regular updates should be performed
C. Preview screens should be disabled
D. Email client features should be disabled

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**
Internet filter appliances/servers will most likely analyze which three items? (Select THREE).

A. Certificates
B. CRLs
C. Content
D. URLs

**Correct Answer:** ACD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**
Which practice can best code applications in a secure manner?

A. Input validation
B. Object oriented coding
C. Cross-site scripting
D. Rapid Application Development (RAD)

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**
In addition to bribery and forgery, which of the following are the MOST common techniques that attackers use to socially engineer people? (Select TWO)

A. Phreaking
B. Dumpster diving
C. Whois search
D. Flattery
E. Assuming a position of authority

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**
Which of the following will restrict access to files according to the identity of the user or group?

A. MAC
B. CRL
C. pki
D. DAC

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
Which of the following would be an easy way to determine whether a secure web page has a valid certificate?

A. Right click on the lock at the bottom of the browser and check the certificate information
B. ContactThawte or Verisign and ask about the web page
C. Contact the web page's web master
D. Ensure that the web URL starts with 'https:\\'.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
Which description is correct concerning the process of comparing cryptographic hash functions of system executables, configuration files, and log files?

A. File integrity auditing
B. Stateful packet filtering
C. Host based intrusion detection
D. Network based intrusion detection

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 36**
While hardening an operating system, which item is LEAST effective?

A. Configuration baselines
B. Limiting administrative privileges
C. Installing HIDS
D. Install a software firewall

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
Which of the following types of attacks is BEST described as an attacker capturing part of a communication and later sending that communication segment to the server while pretending to be the client?

A. TCP/IP hijacking
B. Replay
C. Back door
D. Man in the middle

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 38**
Malicious code that enters a target system, lays dormant until a user opens the certain program then deletes the contents of attached network drives and removable storage devices is known as
a:

A. worm
B. Trojan horse
C. logic bomb
D. honeypot

**Correct Answer:** C
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 39**
Which action should be performed when discovering an unauthorized wireless access point attached to a network?

A. Unplug the Ethernet cable from the wireless access point.
B. Change the SSID on the wireless access point
C. Run a ping against the wireless access point.
D. Enable MAC filtering on the wireless access point.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**
Which of the following network authentication protocols uses symmetric key cryptography, stores a shared key for each network resource and uses a Key Distribution Center (KDC)?

A. RADIUS
B. TACACS+
C. Kerberos
D. pki

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**
In cryptography, MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321), MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. A user sees an MD5 hash number beside a file that they wish to download. Which description is true about a hash?

A. A hash is a unique number that is generated after the file has been encrypted and used as the SSL key during download.
B. A hash is a unique number that is generated based upon the TCP/IP transmission header and should be verified before download.
C. A hash is a unique number that is generated based upon the files contents and used as the SSL key during download.
D. A hash is a unique number that is generated based upon the files contents and should be verified after download.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**Exam E**

**QUESTION 1**
When a new network device is configured for first-time installation, which of the following is a security threat?

A. Denial of Service (DoS)
B. Attacker privilege escalation
C. Installation of a back door
D. Use of default passwords

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 2**
Which of the following access control models uses subject and object labels?

A. Mandatory Access Control (MAC)
B. Role Based Access Control (RBAC)
C. Rule Based Access Control (RBAC)
D. Discretionary Access Control (DAC)

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 3**
Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Which of the following is considered the weakest encryption?

A. 5HA
B. DES
C. RSA
D. AES

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
Which of the following access decisions are based on a Mandatory Access Control (MAC) environment?

A. Access control lists
B. Ownership
C. Group membership
D. Sensitivity labels

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
Audit log information can BEST be protected by: (Select TWO).

A. using a VPN
B. an IDS
C. access controls that restrict usage
D. an intrusion prevention system (IPS)
E. recording to write-once media.
F. a firewall that creates an enclave

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
Which method will most effectively verify that a patch file downloaded from a third party has not been modified since the time that the original manufacturer released the patch?

A. Compare the final MD5 hash with the original.
B. Compare the final LANMAN hash with the original.
C. Download the patch file through a SSL connection.
D. Download the patch file over an AES encrypted VPN connection.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 7**
Non-essential services are often appealing to attackers because non-essential services: (Select TWO)

A. consume less bandwidth
B. are not visible to an IDS
C. provide root level access
D. decrease the surface area for the attack
E. are not typically configured correctly or secured
F. sustain attacks that go unnoticed

**Correct Answer:** EF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
Which action should be performed to harden workstations and servers?

A. Report all security incidents.
B. Install only needed software.
C. Log on only as the administrator.
D. Check the logs regularly.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 9**
John works as a network administrator for his company. He uses a tool to check SMTP, DNS, P0P3, and ICMP packets on the network. This is an example of which of the following?

A. A vulnerability scan
B. A protocol analyzer
C. A penetration test
D. A port scanner

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 10**
Which of the following types of malicious software travels across computer networks without requiring a user to distribute the software?

A. Virus
B. Worm
C. Trojan horse
D. Logic bomb

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
What will be implemented by a technician to mitigate the chances of a successful attack against the wireless network?

A. Implement an authentication system and WEP.

B. Implement an identification system and WPA2.
C. Implement an authentication system and WPA.
D. Implement a biometric system and WEP.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
Which of the following should be done if an audit recording fails in an information system?

A. Log off the user
B. Overwrite the oldest audit records
C. Stop generating audit records
D. Send an alert to the appropriate personnel

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
Which of the following types of authentication BEST describes providing a username, password and undergoing a thumb print scan to access a workstation?

A. Multifactor
B. Mutual
C. Biometric
D. Kerberos

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
Which item specifies a set of consistent requirements for a workstation or server?

A. Patch management
B. Vulnerability assessment
C. Imaging software
D. Configuration baseline

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
Which of the following steps is MOST often overlooked during the auditing process?

A. Reviewing event logs regularly
B. Enabling auditing on the system
C. Auditing every system event
D. Deciding what events to audit

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 16**
Kerberos uses which of the following ports by default?

A. 23
B. 88
C 139
C. 443

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
What should be taken into consideration while executing proper logging procedures? (Select TWO).

A. The information that is needed to reconstruct events
B. The password requirements for user accounts
C. The virtual memory allocated on the log server
D. The amount of disk space required

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
Turnstiles, double entry doors and security guards are all prevention measures for which of the following types of social engineering?

A. Piggybacking
B. Looking over a co-workersshould'er to retrieve information
C. Looking through a co-worker's trash to retrieve information
D. Impersonation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 19**
Alex is a network administrator of his company. He is backing up all server data nightly to a local NAS device. Which additional action should Alex perform to block disaster in the case the primary site is permanently lost?

A. Backup all data at a preset interval to removable disk and store the disk in a fireproof safe in the buildings basement.
B. Backup all data at a preset interval to tape and store those tapes at a sister site in another city.
C. Backup all data at a preset interval to tape and store those tapes at a sister site across the street.
D. Backup all data at a preset interval to removable disk and store the disk in a safety deposit box at theadministrators home.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
Which of the following programming techniques should be used to prevent buffer overflow attacks?

A. Input validation
B. Nested loops
C. Signed applets
D. Automatic updates

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
Which of the following authentication systems make use of the KDC Key Distribution Center?

A. Certificates
B. Security Tokens
C. CHAP
D. Kerberos

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
A digital signature or digital signature scheme is a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which of the following keys?

A. Senders public key
B. Receivers private key
C. Receivers public key
D. Senders private key

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
Users need to access their email and several secure applications from any workstation on the network. In addition, an authentication system implemented by the administrator requires the use of a username, password, and a company issued smart card. This is an example of which of the following?

A. Three factor authentication
B. SSO
C. ACL
D. Least privilege

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
Which of the following statements regarding authentication protocols is FALSE?

A. PAP is insecure because usernames and passwords are sent over the network in clear text.
B. CHAP is more secure than PAP because it encrypts usernames and passwords before they are sent over the network.
C. RADIUS is a client/server-based system that provides authentication, authorization, and accounting services for remote dial-up access.
D. MS-CHAP version 1 is capable of mutual authentication of both the client and the server.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 25**
Which password management system best provides for a system with a large number of users?

A. Self service password reset management systems

B. Locally saved passwords management systems
C. multiple access methods management systems
D. synchronized passwords management systems

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 26**
Why will a Faraday cage be used?

A. To find rogue access points
B. To allow wireless usage
C. To mitigate data emanation
D. To minimize weak encryption

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 27**
Which definition best defines what a challenge-response session is?

A. A challenge-response session is a workstation or system that produces a random challenge string that the user provides, when prompted, in conjunction with the proper PIN (Personal Identification Number).
B. A challenge-response session is a workstation or system that produces a random login ID that the user provides, when prompted, in conjunction with the proper PIN (Personal Identification Number).
C. A challenge-response session is a special hardware device used to produce random text in a cryptography system.
D. A challenge-response session is the authentication mechanism in the workstation or system that does not determine whether the owner should be authenticated.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
The hashing algorithm is created from a hash value, making it nearly impossible to derive the original input number. Which item can implement the strongest hashing algorithm?

A. NTLMv2
B. LANMAN
C. NTLM
D. VLAN

**Correct Answer:** A

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
For which reason are clocks used in Kerberos authentication?

A. Clocks are used to ensure proper connections.
B. Clocks are used to ensure that tickets expire correctly.
C. Clocks are used to generate the seed value for the encryptions keys.
D. Clocks are used to both benchmark and specify the optimal encryption algorithm.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**
Network utilization is the ratio of current network traffic to the maximum traffic that the port can handle. Which of the following can most effectively determine whether network utilization is abnormal?

A. Application log
B. Performance baseline
C. Systems monitor
D. Security log

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**
To reduce vulnerabilities on a web server, an administrator should adopt which of the following preventative measures?

A. Use packet sniffing software on all inbound communications
B. Apply the most recent manufacturer updates and patches to the server.
C. Enable auditing on the web server and periodically review the audit logs
D. Block all Domain Name Service (DNS) requests coming into the server.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**
A travel reservation organization conducts the majority of its transactions via a public facing website. Any downtime to this website will lead to serious financial damage for this organization. One web server is

connected to several distributed database servers. Which statement is correct about this scenario?

A. RAID
B. Warm site
C. Proxy server
D. Single point of failure

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**
Which of the following is a common type of attack on web servers?

A. Birthday
B. Buffer overflow
C. Spam
D. Brute force

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. When an IDS is configured to match a specific traffic pattern, then which of the following is this referring to?

A. Signature-based
B. Behavior-based
C. Anomaly-based
D. Heuristic-based

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
The employees at a company are using instant messaging on company networked computers. The MOST important security issue to address when using instant messaging is that instant messaging:

A. communications are a drain on bandwidth
B. communications are open and unprotected
C. has no common protocol
D. uses weak encryption

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 36**
Removable storage has been around almost as long as the computer itself. Which of the following is the GREATEST security risk regarding removable storage?

A. Availability of data
B. Integrity of data
C. Not enough space available
D. Confidentiality of data

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
A VPN typically provides a remote access link from one host to another over:

A. an intranet
B. a modem
C. a network interface card
D. the Internet

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 38**
In which authentication model a ticket granting server is an important concept?

A. CHAP
B. pap
C. Kerberos
D. RADIUS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 39**
Which of the following would be needed to ensure that a user who has received an email cannot claim that the email was not received?

A. Anti-aliasing
B. Data integrity
C. Asymmetric cryptography
D. Non-repudiation

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**
Coaxial cable is a cable consisting of an inner conductor, surrounded by a tubular insulating layer typically made from a flexible material with a high dielectric constant, all of which is then surrounded by another conductive layer (typically of fine woven wire for flexibility, or of a thin metallic foil), and then finally covered again with a thin insulating layer on the outside. Which is the primary security risk with coaxial cable?

A. Crosstalk between the wire pairs
B. Data emanation from the core
C. Refraction of the signal
D. Diffusion of the core light source

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**
Which of the following portions of a company's network is between the Internet and an internal network?

A. IDS
B. Demilitarized zone (DMZ)
C. Filter router
D. Bastion host

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 42**
A technician is conducting a forensics analysis on a computer system. Which step should be taken FIRST?

A. Search for Trojans.
B. Look for hidden files.
C. Get a binary copy of the system.
D. Analyze temporary files.

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 43**
Which of the following is MOST often used to allow a client or partner access to a network?

A. Extranet
B. Intranet
C. VLAN
D. Demilitarized zone (DMZ)

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 44**
In a secure environment, which authentication mechanism will perform better?

A. RADIUS because it encrypts client-server passwords.
B. TACACS because it encrypts client-server negotiation dialogs.
C. TACACS because it is a remote access authentication service.
D. RADIUS because it is a remote access authentication service.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 45**
Which of the following types of firewalls provides inspection at layer 7 of the OSI model?

A. Application-proxy
B. Network address translation (NAT)
C. Packet filters
D. Stateful inspection

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 46**
Which goals can be achieved by use of security templates? (Select TWO).

A. To ensure that PKI will work properly within thecompanys trust model

B. To ensure that performance is standardized across all servers
C. To ensure that servers are in compliance with the corporate security policy
D. To ensure that all servers start from a common security configuration

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 47**
A newly hired security specialist is asked to evaluate a company's network security. The security specialist discovers that users have installed personal software; the network OS has default settings and no patches have been installed and passwords are not required to be changed regularly. Which of the following would be the FIRST step to take?

A. Install software patches.
B. Disable non-essential services.
C. Enforce the security policy.
D. Password management

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**Exam F**

**QUESTION 1**
Which of the following can be used to implement a procedure to control inbound and outbound traffic on a network segment?

A. Proxy
B. NIDS
C. ACL
D. HIDS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 2**
Giving each user or group of users only the access they need to do their job is an example of which of the following security principals?

A. Least privilege
B. Defense in depth
C. Separation of duties
D. Access control

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 3**
In computing, the Basic Input/Output System (BIOS , also known as the System BIOS, is a de facto standard defining a firmware interface for IBM PC Compatible computers. A user is concerned with the security of their laptops BIOS. The user would not like anyone to be able to access control functions except themselves. Which of the following could make the BIOS more secure?

A. Password
B. Flash the BIOS
C. Encrypt the hard drive
D. Create an access-list

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
A company is upgrading the network and needs to reduce the ability of users on the same floor and network segment to see each other's traffic. Which of the following network devices should be used?

A. Router
B. Hub
C. Switch
D. Firewall

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
In computing, a Uniform Resource Locator (URL) is a type of Uniform Resource Identifier (URI) that specifies where an identified resource is available and the mechanism for retrieving it. When a user attempts to go to a website, he notices the URL has changed, which attack will MOST likely cause the problem?

A. ARP poisoning
B. DLL injection
C. DNS poisoning
D. DDoS attack

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
A system administrator reports that an unauthorized user has accessed the network. Which of the following would be the FIRST action to take?

A. Notify management.
B. Determine the business impact.
C. Contact law enforcement officials.
D. Contain the problem.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 7**
After analyzing vulnerability and applying a security patch, which non-intrusive action should be taken to verify that the vulnerability was truly removed?

A. Update the antivirus definition file.
B. Apply a security patch from the vendor.
C. Repeat the vulnerability scan.
D. Perform a penetration test.

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
A companys security' specialist is securing a web server that is reachable from the Internet. The web server is located in the core internal corporate network. The network cannot be redesigned and the server cannot be moved. Which of the following should the security specialist implement to secure the web server? (Select TWO).

A. Router with an IDS module
B. Network-based IDS
C. Router with firewall rule set
D. Host-based IDS
E. Network-basedfirewal
F. Host-based firewall

**Correct Answer:** DF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 9**
A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Which method can be used to perform denial of service (DoS) attacks?

A. Adware
B. Botnet
C. Spyware
D. Privilege escalation

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 10**
The CHAP (Challenge Handshake Authentication Protocol) sends a logon request from the client to the server, and the server sends a challenge back to the client At which stage does the CHAP protocol perform the handshake process? Choose the best complete answer.

A. At the stage when the connection is established and at whichever time after the connection has been established.
B. At the stage when the connection is established and when the connection is disconnected.
C. At the stage when the connection is established.
D. At the stage when the connection is disconnected.

**Correct Answer:** A
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 11**
Which of the following are nonessential protocols and services?

A. Network News Transfer Protocol (NNTP)
B. TFTP (Trivial File Transfer Protocol).
C. Domain Name Service (DNS)
D. Internet Control Message Protocol (ICMP)

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
Which of the following protocols are not recommended due to them supplying passwords and information over the network?

A. Network News Transfer Protocol (NNTP)
B. SNMP (Simple Network Management Protocol).
C. Domain Name Service (DNS)
D. Internet Control Message Protocol (ICMP)

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
Most key fob based identification systems use which of the following types of authentication mechanisms? (Select TWO).

A. Kerberos
B. Biometrics
C. Username/password
D. Certificates
E. Token

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
Which item will MOST likely permit an attacker to make a switch function like a hub?

A. MAC flooding
B. DNS spoofing
C. ARP poisoning
D. DNS poisoning

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
Which of the following describes a server or application that is accepting more input than the server or application is expecting?

A. Denial of service (DoS)
B. Syntax error
C. Buffer overflow
D. Brute force

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 16**
The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams (hereafter referred to as just "authentication"), and to provide protection against replays. Which of the following is correct about authentication headers (AH)?

A. The authentication information is a keyed hash based on all of the bytes in the packet.
B. The authentication information may be the same on different packets if the integrity remains in place.
C. The authentication information hash will increase by one if the bytes remain the same on transfer.
D. The authentication information hash will remain the same if the bytes change on transfer.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
Which of the following refers to the ability to be reasonably certain that data is not modified or tampered with?

A. Authentication
B. Integrity
C. Non-repudiation
D. Confidentiality

**Correct Answer:** B
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 18**
Disguising oneself as a reputable hardware manufacturer's field technician who is picking up a server for repair would be described as:

A. a phishing attack
B. a Trojan horse
C. a man-in-the-middle attack
D. social engineering

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 19**
A graphical user interface (GUI) is a type of user interface which allows people to interact with electronic devices such as computers; hand-held devices such as MP3 Players, Portable Media Players or Gaming devices; household appliances and office equipment. Which of the following will allow a technician to restrict a user accessing to the GUI?

A. Use of logical tokens
B. Group policy implementation
C. Password policy enforcement
D. Access control lists

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
A security specialist has downloaded a free security software tool from a trusted industry site. The source has published the MD5 hash values for the executable program. The specialist performs a successful virus scan on the download but the MD5 hash is different. Which of the following steps should the specialist take?

A. Avoid executing the file and contact the source website administrator
B. Ignore the MD5 hash values because the values can change during IP fragmentation.
C. Re-run the anti-virus program to ensure that it contains no virus execute
D. Install the executable program because there was probably a mistake with the MD5 value.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
Which of the following can be used by a technician to detect staff members that are connecting to an unauthorized website?

A. Protocol analyzer
B. Host routing table
   C HIDS
C. Bluesnarfing

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
Which of the following would be the BEST reason to disable unnecessary services on a server?

A. Not starting a service will save system memory and reduce startup time.
B. If a service doesn't support the function of the server the service won't be missed.
C. Attack surface and opportunity for compromise are reduced
D. Services can be re-enabled if needed at a later time

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
Access controls based on security labels associated with each data item and each user are known as:

A. Mandatory Access Control (MAC)
B. Role Based Access Control (RBAC)
C. List Based Access Control (LBAC)
D. Discretionary Access Control (DAC)

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
Which tool can help the technician to find all open ports on the network?

A. Router ACL
B. Performance monitor
C. Protocol analyzer
D. Network scanner

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 25**
A user is assigned access rights explicitly. This is a feature of which of the following access control models?

A. Discretionary Access Control (DAC)
B. Mandatory Access Control (MAC)
C. Rule Based Access Control (RBAC)
D. Role Based Access Control (RBAC)

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 26**
Which algorithms can best encrypt large amounts of data?

A. Asymmetric key algorithms
B. Symmetric key algorithms
C. ECC algorithms
D. Hashing algorithms

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 27**
Which of the following describes an attacker encouraging a person to perform an action in order to be successful?

A. Man-in-the-middle
B. Social engineering
C. Back door
D. Password guessing

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
During which phase of identification and authentication does proofing occur?

A. Authentication
B. Testing
C. Verification
D. Identification

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
Which item can reduce the attack surface of an operating system?

A. Installing HIDS
B. Patch management
C. Installing antivirus
D. Disabling unused services

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**
Which of the following connectivity is required for a web server that is hosting an SSL based web site?

A. Port 443 inbound
B. Port 443 outbound
C. Port 80 inbound
D. Port 80 outbound

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**
For the following items, which is a protocol analyzer?

A. Cain _Abel
B. WireShark
C. Nessus
D. John the Ripper

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**
Malicious port scanning is a method of attack to determine which of the following?

A. Computer name
B. The fingerprint of the operating system
C. The physical cabling topology of a network
D. User IDs and passwords

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**
Which of the following is used to determine equipment status and modify the configuration or settings of network devices?

A. SNMP
B. DHCP
C SMTP
C. CHAP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
Which item will effectively allow for fast, highly secure encryption of a USB flash drive?

A. 3DES
B. SHA-1
C. MD5
D. AES256

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
Which of the following describes the process by which a single user name and password can be entered to access multiple computer applications?

A. Single sign-on
B. Encryption protocol
C. Access control lists

D. Constrained user interfaces

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 36**
To preserve evidence for later use in court, which of the following needs to be documented?

A. Audit trail of systems usage
B. Disaster recovery plan
C. Chain of certificates
D. Chain of custody

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
What are best practices while installing and securing a new system for a home user? (Select THREE).

A. Use a strong firewall.
B. Install remote control software.
C. Apply all system patches.
D. Apply all service packs.

**Correct Answer:** ACD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 38**
Which of the following is a major reason that social engineering attacks succeed?

A. Strong passwords are not required
B. Lack of security awareness
C. Multiple logins are allowed
D. Audit logs are not monitored frequently

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 39**
Which of the following types of backups requires that files and software that have been changed since the last

full backup be copied to storage media?

A. Incremental
B. Differential
C. Full
D. Delta

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**
Which port must be open to allow a user to login remotely onto a workstation?

A. 53
B. 636
C. 3389
D. 8080

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**
The authentication process where the user can access several resources without the need for multiple credentials is known as:

A. Discretionary Access Control (DAC).
B. need to know
C. decentralized management
D. single sign-on

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 42**
Which item best describes an instance where a biometric system identifies legitimate users as being unauthorized?

A. False acceptance
B. False positive
C. False rejection
D. False negative

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**Exam G**

**QUESTION 1**
Which of the following is the best description about the method of controlling how and when users can connect in from home?

A. Remote access policy
B. Remote authentication
C. Terminal access control
D. Virtual Private Networking (VPN)

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 2**
Which of the following would be the MOST common method for attackers to spoof email?

A. Web proxy
B. Man in the middle attacks
C. Trojan horse programs
D. Open relays

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 3**
The implicit deny will block anything you didn't specifically allow but you may have allowed stuff that you don't need. A technician is reviewing the system logs for a firewall and is told that there is an implicit deny within the ACL Which is an example of an implicit deny?

A. An implicitdeny statement denies all traffic from one network to another.
B. Each item is denied by default because of the implicit deny.
C. Items which are not specifically given access are denied by default.
D. An ACL is a way to secure traffic from one network to another.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
Which of the following is often misused by spyware to collect and report a user's activities?

A. Persistent cookie
B. Web bug

C. Tracking cookie
D. Session cookie

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
Choose the figure which represents the number of ports in the TCP/IP (Transmission Control Protocol/Internet Protocol) which are vulnerable to being scanned, attacked, and exploited.

A. 32 ports
B. 1,024 ports
C. 65,535 ports
D. 16,777,216 ports

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
Tom is a network technician of his company. Now, he is making a decision between implementing a HIDS on the database server and implementing a NIDS. Why NIDS may be better to implement? (Select TWO).

A. Many HIDS only offer a low level of detection granularity.
B. Many HIDS are not able to detect network attacks.
C. Many HIDS have a negative impact on system performance.
D. Many HIDS are not good at detecting attacks on database servers.

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 7**
Which of the following would be considered a detrimental effect of a virus hoax? (Select TWO).

A. The email server capacity is consumed by message traffic.
B. Technical support resources are consumed by increased user calls.
C. Users are tricked into changing the system configuration.
D. Users are at risk for identity theft.

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
To keep an 802.llx network from being automatically discovered, a user should:

A. turn off the SSID broadcast
B. leave the SSID default.
C. change the SSID name.
D. activate the SSID password

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 9**
Which security policy will be most likely used while attempting to mitigate the risks involved with allowing a user to access company email via their cell phone?

A. The cell phone should require a password after a set period of inactivity.
B. The cell phone should have data connection abilities disabled.
C. The cell phone should only be used for company related emails.
D. The cell phone data should be encrypted according to NIST standards.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 10**
Which of the following BEST describes the baseline process of securing devices on a network infrastructure?

A. Enumerating
B. Hardening
C. Active prevention
D. Passive detection

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
Which of the following types of removable media is write-once and appropriate for archiving security logs?

A. Tape
B. CD-R
C. Hard disk
D. USB drive

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
After installing new software on a machine, what needs to be updated to the baseline?

A. Honeypot
B. Signature-based NIPS
C. Signature-based NIDS
D. Behavior-based HIDS

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
A PC is rejecting push updates from the server; all other PCs on the network are accepting the updates successfully. What should be examined first?

A. Password expiration
B. Local firewall
C. Anti-spyware
D. Pop-up blocker

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
A company wants to connect the network to a manufacturer's network to be able to order parts. Which of the following types of networks should the company implement to provide the connection while limiting the services allowed over the connection?

A. Scatternet
B. Extranet
C. VPN
D. Intranet

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
Malware, a portmanteau from the words malicious and software, is software designed to infiltrate or damage a computer system without the owner's informed consent. A network technician suspects that a piece of malware is consuming too many CPU cycles and slowing down a system. Which item can help determine the amount of CPU cycles being consumed?

A. Install malware scanning software.
B. Run performance monitor to evaluate the CPU usage.
C. Use a protocol analyzer to find the cause of the traffic.
D. Install HIDS to determine the CPU usage.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 16**
Which of the following ports are typically used by email clients? (Select TWO)

A. 3389
B. 194
C. 143
D. 110
E. 49
F. 23

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
Fiber optic cable is considered safer than CAT5 because fiber optic cable: (Select TWO).

A. is not susceptible to interference.
B. is hard to tap in to.
C. is made of glass rather than copper.
D. can be run for a longer distance
E. is more difficult to install

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
A DNS (Domain Name Service) server uses a specific port number. Choose this port number from the options.

A. Port 32

B. Port 1,024
C. Port 65,535
D. Port 16,777,216

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 19**
Which of the following access attacks would involve looking through your files in the hopes of finding something interesting?

A. Interception
B. Snooping
C. Eavesdropping
D. None of the above

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
A company wants to implement a VLAN. Senior management believes that a VLAN will be secure because authentication is accomplished by MAC addressing and that dynamic trunking protocol (DTP) will facilitate network efficiency. Which of the following issues should be discussed with senior management before VLAN implementation?

A. MAC addresses can be spoofed and DTP allows rogue network devices to configure ports
B. MAC addresses can be spoofed and DTP allows only authenticated users.
C. MAC addresses are a secure authentication mechanism and DTP allows rogue network devices to configure ports.
D. MAC addresses are a secure authentication mechanism and DTP allows only authenticated users.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
John works as a network administrator for his company. On the monthly firewall log, he discovers that many internal PCs are sending packets on a routine basis to a single external PC. Which statement correctly describes what is happening?

A. The remote PC has a zombie slave application running and the local PCs have a zombie master application running.
B. The remote PC has a zombie master application running and the local PCs have a zombie slave application running.
C. The remote PC has a spam slave application running and the local PCs have a spam master application

running.

D. The remote PC has a spam master application running and the local PCs have a spam slave application running.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
Which key can be used by a user to log into their network with a smart card?

A. Public key
B. Cipher key
C. Shared key
D. Privatekey

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
Which description is true about the process of securely removing information from media (e.g. hard drive) for future use?

A. Deleting
B. Reformatting
C. Sanitization
D. Destruction

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
Which of the following provides the MOST secure form of encryption?

A. 3DES
B. Diffie-Hellman
C. DES
D. AES

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 25**
Users on a network report that they are receiving unsolicited emails from the same email address. Which action should be performed to prevent this from occurring?

A. Install an ACL on the firewall to block traffic from the sender and filter the IP address.
B. Configure a rule in eachusers router and restart the router.
C. Install an anti-spam filter on the domain mail servers and filter the email address.
D. Configure rules on the users host and restart the host.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 26**
Which of the following describes the validation of a message's origin?

A. Integrity
B. Confidentiality
C. Non-repudiation
D. Asymmetric encryption

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 27**
Users are using thumb drives to connect to USB ports on company workstations. A technician is concerned that sensitive files can be copied to the USB drives. Which mitigation technique would address this concern? (Select TWO).

A. Disable the USB root hub within the OS.
B. Apply the concept of least privilege to USB devices.
C. Disable USB within the workstations BIOS.
D. Run spyware detection against all workstations.

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
Using software on an individual computer to generate a key pair is an example of which of the following approaches to PKI architecture?

A. Decentralized
B. Centralized

C. Hub and spoke
D. Distributed key

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
Which description is true about how to accomplish steganography in graphic files?

A. Replacing the most significant bit of each byte
B. Replacing the most significant byte of each bit
C. Replacing the least significant byte of each bit
D. Replacing the least significant bit of each byte

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**
Which of the following types of encryption would be BEST to use for a large amount of data?

A. Asymmetric
B. Symmetric
C. ROT13
D. Hash

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**
Which one of the following options is a vulnerability assessment tool?

A. AirSnort
B. John the Ripper
C. Cain _Abel
D. Nessus

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**
Malicious software that travels across computer networks without user assistance is an example of a:

A. worm
B. virus
C. logic bomb
D. Trojan hors

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**
You work as a network administrator for your company. Your company has just detected a malware incident. Which will be your first response?

A. Removal
B. Containment
C. Recovery
D. Monitor

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
When setting password rules, which of the following would lower the level of security of a network?

A. Passwords must be greater than six characters and contain at least one non-alpha.
B. All passwords are set to expire at regular intervals and users are required to choose new passwords that have not been used before.
C. Complex passwords that users can not remotely change are randomly generated by the administrator and given to users
D. After a set number of failed attempts the server will lock out any user account forcing the user to call the administrator to re-enable the account.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
You are a network technician of your company. You have just detected an intrusion on your company??s network from the Internet. What should be checked FIRST?

A. The firewall logs
B. The performance logs

C. The DNS logs
D. The access logs

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 36**
A person pretends to be a telecommunications repair technician, enters a building stating that there is a networking trouble work order and requests that a security guard unlock the wiring closet The person connects a packet sniffer to the network switch in the wiring closet and hides the sniffer behind the switch against a wall. This is an example of:

A. a vulnerability scan
B. social engineering
C. a man in the middle attack
D. a penetration test

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
Which method could identify when unauthorized access has occurred?

A. Implement session termination mechanism.
B. Implement previous logon notification.
C. Implement session lock mechanism.
D. Implement two-factor authentication.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 38**
Which of the following definitions would be correct regarding Eavesdropping?

A. Placing a computer system between the sender and receiver to capture information.
B. Someone looking through your files.
C. Listening or overhearing parts of a conversation
D. Involve someone who routinely monitors network traffic.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 39**
Which practice is the best to secure log files?

A. Copy or save the logs to a remote log server.
B. Change security settings to avoid corruption.
C. Log all failed and successful login attempts.
D. Deny administrators all access to log files to prevent write failures.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**
Which of the following definitions would be correct regarding Active Inception?

A. Someone looking through your files
B. Involve someone who routinely monitors network traffic
C. Listening or overhearing parts of a conversation
D. Placing a computer system between the sender and receiver to capture information.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**
How to test the integrity of a company's backup data?

A. By reviewing the written procedures
B. By conducting another backup
C. By restoring part of the backup
D. By using software to recover deleted files

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 42**
Nmap has been run against a server and more open ports than expected have been discovered. Which of the following would be the FIRST step to take?

A. All ports should be closed and observed to see whether a process tries to reopen the port.
B. Nmap should be run again and observed to see whether different results are obtained.
C. All ports should be left open and traffic monitored for malicious activity

D. The process using the ports should be examined.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 43**
Which statement best describes a static NAT?

A. A static NAT uses a many to many mapping.
B. A static NAT uses a one to many mapping.
C. A static NAT uses a many to one mapping.
D. A static NAT uses a one to one mapping.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 44**
Which of the following would be MOST desirable when attacking encrypted data?

A. Sniffed traffic
B. Block cipher
C. Weak key
D. Algorithm used

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 45**
Which scanner can find a rootkit?

A. Email scanner
B. Malware scanner
C. Anti-spam scanner
D. Adware scanner

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 46**
From the listing of attacks, choose the attack which exploits session initiation between a Transport Control

Program (TCP) client and server within a network?

A. Buffer Overflow attack
B. SYN attack
C. Smurf attack
D. Birthday attack

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**Exam H**

**QUESTION 1**
A technician reports that an employee that retired five years ago still has access to the marketing department's folders. Which of the following should have been conducted to avoid this security risk?

A. Job rotation review
B. Separation of duties review
C. Retention policy review
D. Regular user access review

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 2**
Social engineering attacks would be MOST effective in which of the following environments? (Select TWO).

A. A locked, windowless building
B. A military facility with computer equipment containing biometrics.
C. A public building that has shared office space.
D. A company with a dedicated information technology (IT) security staff.
E. A company with a help desk whose personnel have minimal training.

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 3**
What is steganography primarily used for?

A. Data integrity
B. Message digest
C. Hide information
D. Encrypt information

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
Which of the following is the MOST effective way for an administrator to determine what security holes reside on a network?

A. Perform a vulnerability assessment
B. Run a port scan

C. Run a sniffer
D. Install and monitoran IDS

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
A company has instituted a VPN to allow remote users to connect to the office. As time progresses multiple security associations are created with each association being more secure. Which of the following should be implemented to automate the selection of the BEST security association for each user?

A. AES
B. 3DES
C. SHA
D. IKE

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
Which item is not a logical access control method?

A. biometrics
B. group policy.
C. ACL
D. software token.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 7**
The concept that a web script is run in its own environment and cannot interfere with any other process is known as a:

A. honey pot
B. VLAN
C. quarantine
D. sandbox

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
Which description is true about the external security testing?

A. Conducted from outside the perimeter switch but inside the border router
B. Conducted from outside the perimeter switch but inside the firewall
C. Conducted from outside the organizations security perimeter
D. Conducted from outside the building that hosts the organizations servers

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 9**
What should be established immediately upon evidence seizure?

A. Forensic analysis
B. Start the incident respond plan
C. Chain of custody
D. Damage and loss control

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 10**
Which of the following uses private key / public key technology to secure web sites?

A. SSL
B. TCP
C. Media Access Control (MAC)
D. Access Control List (ACL)

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
Which one of the following options will permit an attacker to hide the presence of malicious code through altering the systems process and registry entries?

A. Trojan
B. Logic bomb
C. Worm
D. Rootkit

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
Patch management must be combined with full-featured systems management to be effective. Determining which patches are needed, applying the patches and which of the following are three generally accepted activities of patch management?

A. Backing up the patch file executables to a network share
B. Updating the firewall configuration to include the patches
C. Auditing for the successful application of the patches
D. Running a NIDS report to list the remaining vulnerabilities

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
The MOST common exploits of Internet-exposed network services are due to:

A. illicit servers
B. Trojan horse programs
C. active content (e.g. Java Applets)
D. buffer overflows

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
Which of the following would be an example of a hardware device where keys can be stored? (Select TWO).

A. PCI card
B. Smart card
C. PCMCIA card

D. Network interface card (NIC)

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
Encryption is the conversion of data into a form, called a ciphertext that cannot be easily understood by unauthorized people. Which encryption is the strongest by use of mathematical evaluation techniques?

A. 3DES
B. ROT13
C. AES
D. DES

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 16**
Which technology is able to isolate a host OS from some types of security threats?

A. Kiting
B. Virtualization
C. Cloning
D. Intrusion detection

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
Non-repudiation is enforced by which of the following?

A. Secret keys
B. Digital signatures
C. pki
D. Cipher block chaining

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**

Which of the following would be the MOST effective backup site for disaster recovery?

A. Cold site
B. Warm site
C. Hot site
D. Reciprocal agreement

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 19**
Which one of the following options will create a security buffer zone between two rooms?

A. Mantrap
B. Anti-pass back
C DMZ
C. Turnstile

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
Which of the following describes backing up files and software that have changed since the last full or incremental backup?

A. Full backup
B. Differential backup
C. Incremental backup
D. Delta backup

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
Which is the primary objective to implement performance monitoring applications on network systems from a security standpoint?

A. To detect host intrusions from external networks
B. To detect network intrusions from external attackers
C. To detect integrity degradations to network attached storage
D. To detect availability degradations caused by attackers

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
Which of the following can affect heaps and stacks?

A. SQL injection
B. Cross-site scripting
C. Buffer overflows
D. Rootkits

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
An enclosure that prevents radio frequency signals from emanating out of a controlled environment is BEST described as which of the following?

A. Faraday cage
B. Mantrap
C. Grounded wiring frame
D. TEMPEST

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
Which of the following is not a step in the incident response?

A. recovery.
B. repudiation
C. containment
D. eradication

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 25**
In a classified environment, a clearance into a Top Secret compartment only allows access to certain information within that compartment. This is known as

A. dual control.
B. need to know.
C. separation of duties
D. acceptable use.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 26**
On the basis of certain ports, which of the following will allow wireless access to network resources?

A. 802.11a
B. 802.11n
C. 802.lx
D. 802.11g

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 27**
An organization has a hierarchical-based concept of privilege management with administrators having full access, human resources personnel having slightly less access and managers having access to their own department files only. This is BEST described as:

A. Discretionary Access Control (DAC).
B. Rule Based Access Control (RBAC).
C. Mandatory Access Control (MAC)
D. Role Based Access Control (RBAC)

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
Identify the item that can determine which flags are set in a TCP/IP handshake?

A. Networkmapper
B. FIN/RST
C. Protocol analyzer
D. SYN/ACK

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
A representative from the human resources department informs a security specialist that an employee has been terminated. Which of the following would be the BEST action to take?

A. Disable the employee's user accounts and keep the data for a specified period of time.
B. Disable the employee's user accounts and delete all data.
C. Contact the employee's supervisor regarding disposition of user accounts
D. Change the employee's user password and keep the data for a specified period.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**
One of the below options are correct regarding the DDoS (Distributed Denial of Service) attack?

A. Listening or overhearing parts of a conversation
B. Placing a computer system between the sender and receiver to capture information
C. Use of multiple computers to attack a single organization
D. Prevention access to resources by users authorized to use those resources

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**
Why malware that uses virtualization techniques is difficult to detect?

A. The malware may be implementing a proxy server for command and control.
B. A portion of the malware may have been removed by the IDS.
C. The malware may be using a Trojan to infect the system.
D. The malware may be running at a more privileged level than the antivirus software.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**
An SMTP server is the source of email spam in an organization. Which of the following is MOST likely the cause?

A. The administrator account was not secured.

B. X.400 connectors have not been password protected.
C. Remote access to the email application's install directory has not been removed.
D. Anonymous relays have not been disabled.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**
A graphical user interface (GUI) is a type of user interface which allows people to interact with electronic devices such as computers; hand-held devices such as MP3 Players, Portable Media Players or Gaming devices; household appliances and office equipment. Which of the following will permit a technician to restrict a users?? access to the GUI?

A. Use of logical tokens
B. Group policy implementation
C. Password policy enforcement
D. Access control lists

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
Which key is generally applied FIRST to a message digest to provide non-repudiation by use of asymmetric cryptography?

A. Privatekey of the receiver
B. Privatekey of the sender
C. Public key of the sender
D. Public key of the receiver

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
Default passwords in hardware and software should be changed:

A. if a threat becomes known.
B. once each month
C. when the hardware or software is turned on.
D. when the vendor requires it

**Correct Answer:** C
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 36**
Which of the following types of programs autonomously replicates itself across networks?

A. Trojan horse
B. Worm
C. Virus
D. Spyware

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
An accountant has logged onto the company's outside banking website. An administrator uses a TCP/IP monitoring tool to discover that the accountant was actually using a spoofed banking website. What most likely cause this attack? (Select TWO).

A. Altered hosts file
B. Bluesnarfing
C. Networkmapper
D. DNS poisoning

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 38**
Which of the following is employed to allow distrusted hosts to connect to services inside a network without allowing the hosts direct access to the internal networks?

A. VLAN
B. Extranet
C. Demilitarized zone (DMZ)
D. Intranet

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 39**
You work as a network administrator for your company. Your company requires you to improve the physical security of a data center located inside the office building. The data center already maintains a physical access

log and has a video surveillance system. Which additional control can be performed?

A. ACL
B. Defense-in-depth
C. Logical token
D. Mantrap

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**
Which method is the LEAST intrusive to check the environment for known software flaws?

A. Port scanner
B. Vulnerability scanner
C. Penetration test
D. Protocol analyzer

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**
A honeypot is used to:

A. provide an unauthorized user with a place to safely work.
B. give an unauthorized user time to complete an attack.
C. trap attackers in a false network.
D. allow administrators a chance to observe an attack.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 42**
Which item can easily create an unencrypted tunnel between two devices?

A. PPTP
B. AES
C. L2TP
D. HTTPS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 43**
Which of the following are components of host hardening? (Select TWO).

A. Removing a user's access to the user's data.
B. Adding users to the administrator group.
C. Disabling unnecessary services.
D. Configuring the Start menu and Desktop
E. Applying patches

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 44**
Pretty good privacy (PGP) uses a PKI Trust Model where no certificate authority (CA) is subordinate to another. The model with no single trusted root is known as:

A. peer-to-peer.
B. downlevel.
C. hierarchical
D. hybrid

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**Exam I**

**QUESTION 1**
Which statement correctly describes the difference between a secure cipher and a secure hash?

A. A hash can be reversed, a cipher cannot.
B. A hash produces a variable output for any input size, a cipher does not
C. A cipher can be reversed, a hash cannot.
D. A cipher produces the same size output for any input size, a hash does not.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 2**
Which of the following assessment tools would be MOST appropriate for determining if a password was being sent across the network in clear text?

A. Protocol analyzer
B. Port scanner
C. Password cracker
D. Vulnerability scanner

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 3**
A peer-to-peer computer network uses diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather than conventional centralized resources where a relatively low number of servers provide the core value to a service or application. Which of the following is a security risk while using peer-to-peer software?

A. Licensing
B. Cookies
C. Data leakage
D. Multiple streams

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
From the listing of attacks, which analyzes how the operating system (OS) responds to specific network traffic, in an attempt to determine the operating system running in your networking environment?

A. Operating system scanning.

B. Reverse engineering.
C. Fingerprinting
D. Host hijacking.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
For the following items, which one is a collection of servers setup to attract hackers?

A. VLAN
B. DMZ
C. Honeynet
D. Honeypot

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
From the listing of attacks, choose the attack which misuses the TCP (Transmission Control Protocol) three-way handshake process, in an attempt to overload network servers, so that authorized users are denied access to network resources?

A. Man in the middle attack
B. Smurf attack
C. Teardrop attack
D. SYN (Synchronize) attack

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 7**
A technician is helping an organization to correct problems with staff members unknowingly downloading malicious code from Internet websites. Which of the following should the technician do to resolve the problem?

A. Use Java virtual machines to reduce impact
B. Disable unauthorized ActiveX controls
C. Implement a policy to minimize the problem
D. Install a NIDS

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
A protocol analyzer will most likely detect which security related anomalies?

A. Many malformed or fragmented packets
B. Passive sniffing of local network traffic
C. Decryption of encrypted network traffic
D. Disabled network interface on a server

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 9**
One type of network attack sends two different messages that use the same hash function to generate the same message digest. Which network attack does this?

A. Man in the middle attack.
B. Ciphertext only attack.
C. Birthday attack.
D. Brute force attack.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 10**
To which of the following viruses does the characteristic when the virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive, form part of?

A. Polymorphic Virus
B. Trojan Horse Virus
C. Stealth Virus
D. Retrovirus

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
The NIC should be placed in which mode to monitor all network traffic while placing a NIDS onto the network?

A. Promiscuous

B. Half-duplex
C. Full-duplex
D. Auto

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
Which item can be commonly programmed into an application for ease of administration?

A. Back door
B. Trojan
C. Worm
D. Zombie

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
To which of the following viruses does the characteristic when the virus may attempt to infect your boot sector, infect all of your executable files, and destroy your applications files form part of?

A. Multipartite Virus
B. Armored Virus
C. Companion Virus
D. Phage Virus

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
Which of the following is MOST effective in preventing adware?

A. Firewall
B. HIDS
C. Antivirus
D. Pop-up blocker

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
Choose the correct order in which crucial equipment should draw power.

A. Backup generator, UPS battery, UPS line conditioner
B. Uninterruptible Power Supply (UPS) battery, UPS line conditioner, backup generator
C. Backup generator, UPS line conditioner, UPS battery
D. UPS line conditioner, UPS battery, and backup generator

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 16**
Choose the statement that best details the difference between a worm and a Trojan horse?

A. Worms are distributed through e-mail messages while Trojan horses do not.
B. Worms self replicate while Trojan horses do not.
C. Worms are a form of malicious code while Trojan horses are not
D. There is no difference between a worm and a Trojan horse.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
Recently, your company has implemented a work from home program. Employees should connect securely from home to the corporate network. Which encryption technology can be used to achieve this goal?

A. L2TP
B. IPSec
C. pppoE
D. pptp

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
After the maximum number attempts have failed, which of the following could set an account to lockout for 30 minutes?

A. Account lockout threshold
B. Account lockout duration
C. Password complexity requirements

D. Key distribution center

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 19**
Choose the attack or malicious code that cannot be prevented or deterred solely through using technical measures.

A. Dictionary attacks.
B. Man in the middle attacks.
C. DoS (Denial of Service) attacks.
D. Social engineering.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
A Faraday cage or Faraday shield is an enclosure formed by conducting material, or by a mesh of such material. Such an enclosure blocks out external static electrical fields. Faraday cages are named after physicist Michael Faraday, who built one in 1836. Which of the following would a Faraday cage prevent usage of?

A. Cell phone
B. Uninterruptible Power Supply (UPS)
C. Storage drive
D. USB key

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
Which encryption algorithm depends on the inability to factor large prime numbers?

A. SHA-1
B. AES256
C. RSA
D. Elliptic Curve

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
Which solution can be used by a user to implement very tight security controls for technicians that seek to enter the users' datacenter?

A. Combination locks and key locks
B. Smartcard and proximity readers
C. Magnetic lock and pin
D. Biometric reader and smartcard

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
Which of the following is a protocol analyzer?

A. John the Ripper
B. WireShark
C. Cain _Abel
D. Nessus

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
Which of the following common attacks would the attacker capture the user's login information and replay it again later?

A. Back Door Attacks
B. Replay Attack
C. Spoofing
D. ManIn The Middle

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 25**
After auditing file, which log will show unauthorized usage attempts?

A. Application
B. Performance
C. Security
D. System

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 26**
Which of the following encryption algorithms relies on the inability to factor large prime numbers?

A. Elliptic Curve
B. AES256
C. RSA
D. SHA-1

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 27**
While monitoring application activity and modification, which system should be used?

A. NIDS
B. RADIUS
C. HIDS
D. OVAL

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
The difference between identification and authentication is that:

A. authentication verifies a set of credentials while identification verifies the identity of the network.
B. authentication verifies a user ID belongs to a specific user while identification verifies the identity of a user group.
C. authentication verifies a set of credentials while identification verifies the identity of a user requesting credentials.
D. authentication verifies the identity of a user requesting credentials while identification verifies a set of credentials.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
The main objective of risk management in an organization is to reduce risk to a level:

A. where the ALE is lower than the SLE.
B. where the ARO equals the SLE.
C. the organization will mitigate.
D. the organization will accept.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**
Following a disaster, which of the following functions should be returned FIRST from the backup facility to the primary facility?

A. Web services
B. Systems functions
C. Executive functions
D. Least critical functions

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**
PKI to encrypt sensitive emails sent to an assistant. In addition to encrypting the body of the email, the executive wants to encrypt the signature so that the assistant can verify that the email actually came from the executive.

Which asymmetric key should be used by the executive to encrypt the signature?

A. Shared
B. Private
C. Hash
D. Public

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**
Which of the following is a reason to use a vulnerability scanner?

A. To identify open ports on a system
B. To assist with protocol analyzing

C. To identify remote access policies
D. To assist with PKI implementation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**
Your company's website permits customers to search for a product and display the current price and quantity available of each product from the production database. Which of the following will invalidate an SQL injection attack launched from the lookup field at the web server level?

A. NIPS
B. Security template
C. Buffer overflow protection
D. Input validation

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
The FIRST step in creating a security baseline would be:

A. identifying the use case
B. installing software patches
C. vulnerability testing.
D. creating a security policy

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
Look at the following intrusion detection systems carefully, which one uses well defined models of how an attack occurs?

A. Anomaly
B. Protocol
C. Signature
D. Behavior

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 36**
A computer system containing personal identification information is being implemented by a company's sales department. The sales department has requested that the system become operational before a security review can be completed. Which of the following can be used to explain the reasons a security review must be completed?

A. Vulnerability assessment
B. Risk assessment
C. Corporate security policy
D. Need to know policy

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
You work as a network technician. You have been asked to reconstruct the infrastructure of an organization. You should make sure that the virtuaiization technology is implemented securely. What should be taken into consideration while implementing virtuaiization technology?

A. The technician should perform penetration testing on all the virtual servers to monitor performance.
B. The technician should verify that the virtual servers and the host have the latest service packs and patches applied.
C. The technician should verify that the virtual servers are dual homed so that traffic is securely separated.
D. The technician should subnet the network so each virtual server is on a different network segment.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 38**
Which of the following attacks are being referred to if the attack involves the attacker gaining access to a host in the network and logically disconnecting it?

A. TCP/IP Hijacking
B. UDP Attack
C. ICMP Attacks
D. Smurf Attacks

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 39**

Which protocol can be used to ensure secure transmissions on port 443?

A. HTTPS
B. SHTTP
C. Telnet
D. SFTP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**
Which of the following protocols is used to transmit data between a web browser and a web server?

A. SSH
B. HTTP
C. SFTP
D. IMAP4

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**
Which method can be used to correct a single security issue on a workstation?

A. A patch
B. Configuration baseline
C. A service pack
D. Patch management

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 42**
Which of the following logs shows when the workstation was last shutdown?

A. DHCP
B. Security
C. Access
D. System

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 43**
Which one of the following options overwrites the return address within a program to execute malicious code?

A. Buffer overflow
B. Rootkit
C. Logic bomb
D. Privilege escalation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 44**
Which of the following attacks are being referred to if packets are not connection-oriented and do not require the synchronization process?

A. TCP/IP Hijacking
B. UDP Attack
C. ICMP Attacks
D. Smurf Attacks

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 45**
Which security application can not proactively detect workstation anomalies?

A. HIPS
B. NIDS
C. antivirus software
D. personal software firewall.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 46**
One of the below is a description for a password cracker, which one is it?

A. A program that can locate and read a password file.
B. A program that provides software registration passwords or keys.

C. A program that performs comparative analysis.
D. A program that obtains privileged access to the system.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 47**
Risk assessment is a common first step in a risk management process. Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard). As a best practice, risk assessments should be based upon which of the following?

A. An absolute measurement of threats
B. A qualitative measurement of risk and impact
C. A quantitative measurement of risk, impact and asset value
D. A survey of annual loss, potential threats and asset value

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 48**
Which of the below options would you consider as a program that constantly observes data traveling over a network?

A. Smurfer
B. Sniffer
C. Fragmenter
D. Spoofer

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 49**
Which of the following will require setting a baseline? (Select TWO).

A. Anomaly-based monitoring
B. Signature-based monitoring
C. NIPS
D. Behavior-based monitoring

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

## Exam J

**QUESTION 1**
Choose the network mapping tool (scanner) which uses ICMP (Internet Control Message Protocol).

A. A port scanner.
B. A map scanner.
C. A ping scanner.
D. A share scanner.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 2**
One type of port scan can determine which ports are in a listening state on the network, and can then perform a two way handshake. Which type of port scan can perform this set of actions?

A. A TCP (transmission Control Protocol) SYN (Synchronize) scan
B. A TCP (transmission Control Protocol) connect scan
C. A TCP (transmission Control Protocol) fin scan
D. A TCP (transmission Control Protocol) null scan

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 3**
Which one of the following options will allow for a network to remain operational after a Tl failure?

A. Redundant servers
B. Redundant ISP
C. RAID 5 drive array
D. Uninterruptible Power Supply (UPS)

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
Which of the following has largely replaced SLIP?

A. SLIP (Serial Line Internet Protocol)
B. PPP (Point-to-Point Protocol)
C. vpn
D. RADIUS (Remote Authentication Dial-In User Service)

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
Which of the following definitions fit correctly to RADIUS?

A. Is an older protocol that was used in early remote accessenvironments
B. Has largely replaced SLIP and offers multiple protocol support including AppleTalk, IPX, andDECnet
C. are used to make connections between private networks across a public network, such as the Internet
D. is a mechanism that allows authentication of dial-in and other network connections

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
Which description is correct about a tool used by organizations to verify whether or not a staff member has been involved in malicious activity?

A. Mandatory vacations
B. Time of day restrictions
C. Implicit deny
D. Implicit allow

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 7**
Which of the following definitions fit correctly to TACACS?

A. Is an older protocol that was used in early remote accessenvironments
B. Has largely replaced SLIP and offers multiple protocol support including AppleTalk, IPX, andDECnet
C. are used to make connections between private networks across a public network, such as the Internet
D. It allows credentials to be accepted from multiple methods, including Kerberos.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
Which access control method gives the owner control over providing permissions?

A. Mandatory Access Control (MAC)
B. Role-Based Access Control (RBAC)
C. Rule-Based Access control (RBAC)
D. Discretionary Access Control (DAC)

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 9**
Which item best describes an instance where a biometric system identifies legitimate users as being unauthorized?

A. False acceptance
B. False positive
C. False rejection
D. False negative

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 10**
Which of the following definitions fit correctly to PPTP?

A. It supports encapsulation in a single point-to-point environment
B. It was created by Cisco as a method of creating tunnels primarily for dial-up connections
C. It is primarily a point-to-point protocol
D. It is a tunneling protocol originally designed for UNIX systems.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
Which one of the following options is an attack launched from multiple zombie machines in attempt to bring down a service?

A. TCP/IP hijacking
B. DoS
C. DDoS
D. Man-in-the-middle

**Correct Answer:** C
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 12**
From the list of protocols, which two are VPN (Virtual Private Network) tunneling protocols? Choose two protocols.

A. PPP (Point-to-Point Protocol),
B. SLIP (Serial Line Internet Protocol).
C. L2TP (Layer Two Tunneling Protocol).
D. SMTP (Simple Mail Transfer Protocol).
E. PPTP (Point-to-Point Tunneling Protocol).

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
Which of the following is correct about an instance where a biometric system identifies unauthorized users and allows them access?

A. false positive.
B. false rejection.
C. false acceptance.
D. false negative.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
You work as the security administrator at Certkiller.com. You must configure the firewall to support TACACS. Which port(s) should you open on the firewall?

A. Port 21
B. Port 161
C. Port 53
D. Port 49

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
Which security measures should be recommended while implementing system logging procedures? (Select

TWO).

A. Collect system temporary files.
B. Apply retention policies on the log files.
C. Perform CRC checks.
D. Perform hashing of the log files.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 16**
Which of the following network attacks cannot occur in an e-mail attack?

A. Dictionary attack
B. Trojan Horse
C. Phage Virus
D. Polymorphic Virus

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
Which media is LEAST susceptible to a tap being placed on the line?

A. Fiber
B. Coaxial
C. utp
D. STP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
Tom is a network administrator of his company. He suspects that files are being copied to a remote location during off hours. The file server does not have logging enabled. Which logs will be the BEST place to look for information?

A. Antivirus logs
B. Firewall logs
C. DNS logs
D. Intrusion detection logs

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

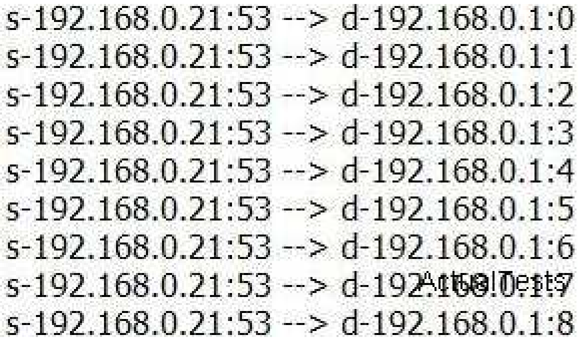
**QUESTION 19**
Job rotation is a cross-training technique where organizations minimize collusion amongst staff.

A. True
B. False

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
A security specialist is reviewing firewall logs and sees the information below. Which of the following BEST describes the attack that is occurring?



```
s-192.168.0.21:53 --> d-192.168.0.1:0
s-192.168.0.21:53 --> d-192.168.0.1:1
s-192.168.0.21:53 --> d-192.168.0.1:2
s-192.168.0.21:53 --> d-192.168.0.1:3
s-192.168.0.21:53 --> d-192.168.0.1:4
s-192.168.0.21:53 --> d-192.168.0.1:5
s-192.168.0.21:53 --> d-192.168.0.1:6
s-192.168.0.21:53 --> d-192.168.0.1:7
s-192.168.0.21:53 --> d-192.168.0.1:8
```

A. ARP poisoning
B. DNS spoofing
C. Port scan
D. PING sweep

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
Which of the following would be MOST useful in determining which internal user was the source of an attack that compromised another computer in its network?

A. The firewall's logs
B. The attacking computer's audit logs
C. The target computer's audit logs.
D. The domain controller's logs.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
Which encryption algorithms can be used to encrypt and decrypt data?

A. NTLM
B. MD5
C. SHA-l
D. RC5

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
By which means do most network bound viruses spread?

A. E-mail
B. Floppy
C. CD-Rom
D. Mass storage devices

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
The Lightweight Directory Access Protocol or LDAP is an application protocol for querying and modifying directory services running over TCP/IP. A user needs to implement secure LDAP on the network. Which port number will secure LDAP use by default?

A. 53
B. 389
C. 443
D. 636

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 25**
Which of the following definitions should BEST suit the functions of an e-mail server?

A. Detect the viruses in the messages received from various sources and send warnings to the recipient to warn him/her of the risky mail.
B. Notify you that a message carries a virus.
C. Forms a platform on which messages are sent.
D. Makes use of a port used specifically for messages to be sent through.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 26**
Choose the primary disadvantage of using a third party mail relay.

A. Spammers can utilize the third party mail relay.
B. A third party mail relay limits access to specific users.
C. A third party mail relay restricts the types of e-mail that maybe sent.
D. A third party mail relay restricts spammers from gaining access.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 27**
Which method is the easiest to disable a 10Base2 network?

A. Remove a vampire tap.
B. Introduce crosstalk.
C. Remove a terminator.
D. Install a zombie.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
Choose the option that details one of the primary benefits of using S/MIME /Secure Multipurpose Internet Mail Extension)?

A. S/MIME allows users to send both encrypted and digitally signed e-mail messages.
B. S/MIME allows users to send anonymous e-mail messages.
C. S/MIME allows users to send e-mail messages with a return receipt.
D. S/MIME expedites the delivery of e-mail messages.

**Correct Answer:** A
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 29**

Host intrusion detection systems (HIDS) and network intrusion detection systems (NIDS) are methods of security management for computers and networks. A HIDS is installed to monitor which of following?

A. Temporary Internet files
B. CPU performance
C. System files
D. NIC performance

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**

On the topic of comparing viruses and hoaxes, which statement is TRUE? Choose the best TRUE statement.

A. Hoaxes can create as much damage as a real virus.
B. Hoaxes are harmless pranks and should be ignored.
C. Hoaxes can help educate users about a virus.
D. Hoaxes carry a malicious payload and can be destructive.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**

The purpose of a DNS server is to enable people and applications to lookup records in DNS tables. Why implement security logging on a DNS server?

A. To monitor unauthorized zone transfers
B. To control unauthorized DNSDoS
C. To measure the DNS server performance
D. To perform penetration testing on the DNS server

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**

Choose the scheme or system used by PGP (Pretty Good Privacy) to encrypt data.

A. Asymmetric scheme

B. Symmetric scheme
C. Symmetric key distribution system
D. Asymmetric key distribution system

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**
Which of the following web vulnerabilities is being referred to when it receives more data than it is programmed to accept?

A. Buffer Overflows.
B. Cookies.
C. cgi.
D. SMTP Relay

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
Which of the following will permit an administrator to find weak passwords on the network?

A. A password generator
B. A networkmapper
C. A hash function
D. A rainbow table

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
Which security measure should be used while implementing access control?

A. Password complexity requirements
B. Disabling SSID broadcast
C. Time of day restrictions
D. Changing default passwords

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 36**
Which of the following web vulnerabilities is being referred to when it has a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers?

A. Buffer Overflows.
B. Cookies.
C. cgi
D. SMTP Relay

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
Study the following items carefully, which one will permit a user to float a domain registration for a maximum of five days?

A. Spoofing
B. DNS poisoning
C. Domain hijacking
D. Kiting

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 38**
A programmer plans to change the server variable in the coding of an authentication function for a proprietary sales application. Which process should be followed before implementing the new routine on the production application server?

A. Change management
B. Secure disposal
C. Password complexity
D. Chain of custody

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 39**
Which of the following definitions BEST suit Buffer Overflow?

A. It receives more data than it is programmed to accept.
B. It is used to provide a persistent, customized web experience for each visit.

C. It's an older form of scripting that was used extensively in early web systems

D. It has a feature designed into many e-mail servers that allows them to forward e-mail to other e- mail servers

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**
An administrator wants to make sure that no equipment is damaged when encountering a fire or false alarm in the server room. Which type of fire suppression system should be used?

A. Carbon Dioxide

B. Deluge sprinkler

C. Hydrogen Peroxide

D. Wet pipe sprinkler

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**
The staff must be cross-trained in different functional areas in order to detect fraud. Which of the following is an example of this?

A. Implicit deny

B. Least privilege

C. Separation of duties

D. Job rotation

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 42**
All of the following provide confidentiality protection as part of the underlying protocol EXCEPT:

A. SSL.

B. SSH.

C. L2TP.

D. IPSeC.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 43**
Which of the following type of attacks would allow an attacker to capture HTTP requests and send back a spoofed page?

A. Teardrop
B. TCP/IP hijacking
C. Phishing
D. Replay

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 44**
Who is finally in charge of the amount of residual risk?

A. The senior management
B. The DRP coordinator
C. The security technician
D. The organizations security officer

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**